IGPS-7084GP

Industrial Managed Ethernet Switch

User's Manual

Version 3.0

Feb, 2013

www.oring-networking.com

COPYRIGHT NOTICE

TRADEMARKS

is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
4F., NO.3, Lane235, Baociao Rd., Sindian City, Taipei County 23145, Taiwan, R.O.C.
Tel: + 886 2 2918 3036 // Fax: + 886 2 2918 3084
Website: www.oring-networking.com

Technical Support
E-mail: support@oring-networking.com

Sales Contact
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

Table of Content

Getting to Know Your Switch

1.1 About the IGPS-7084GP Series Industrial Switch

The IGPS-7084GP series are powerful managed industrial switches which have many features. These switches can work under wide temperature, dusty environment and humid condition. They can be managed by WEB, TELNET, Consol or other third-party SNMP software as well.

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing, RSTP over Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based ,Telnet, Console, CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote Monitoring (RMON)
- 802.3at Power over Ethernet P.S.E

1.3 Hardware Features

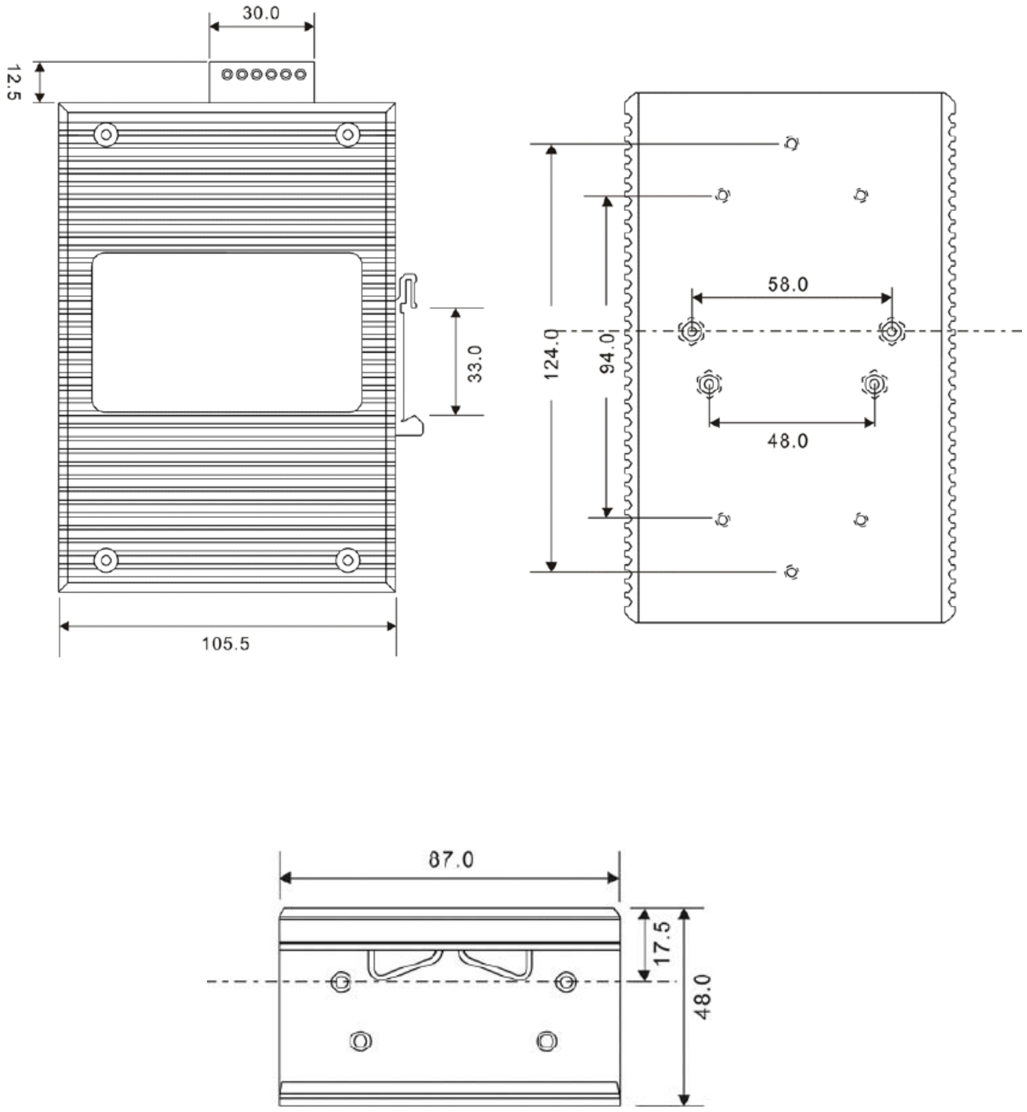
- Redundant DC power inputs
- Operating Temperature: -40 to 70oC
- Storage Temperature: -40 to 85 °C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 8x 1000Base -T
- 4 x 1000 Base-X SFP
- Console Port
- Dimensions 96.4 (W) x 108.5 (D) x 154 (H) mm (3.8 x 4.2.7 x 6.06 inch)

Hardware Installation

2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit on rear panel. The DIN-Rail kit helps switch to fix on the DIN-Rail. It is easy to install the switch on the DIN-Rail:

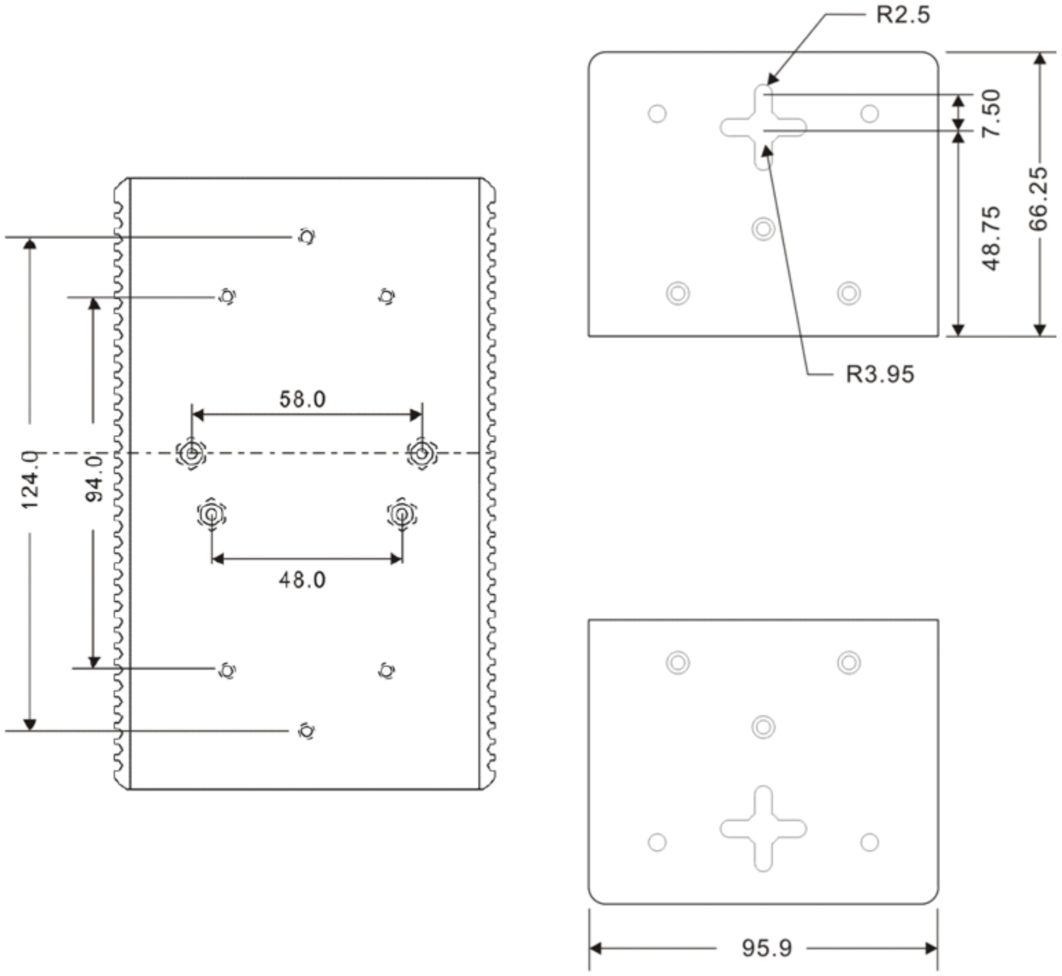
2.1.1 Mount IGPS-7084GP on DIN-Rail



DIN-Rail Size

2.2 Wall Mounting Installation

Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall:



Wall-Mounting size

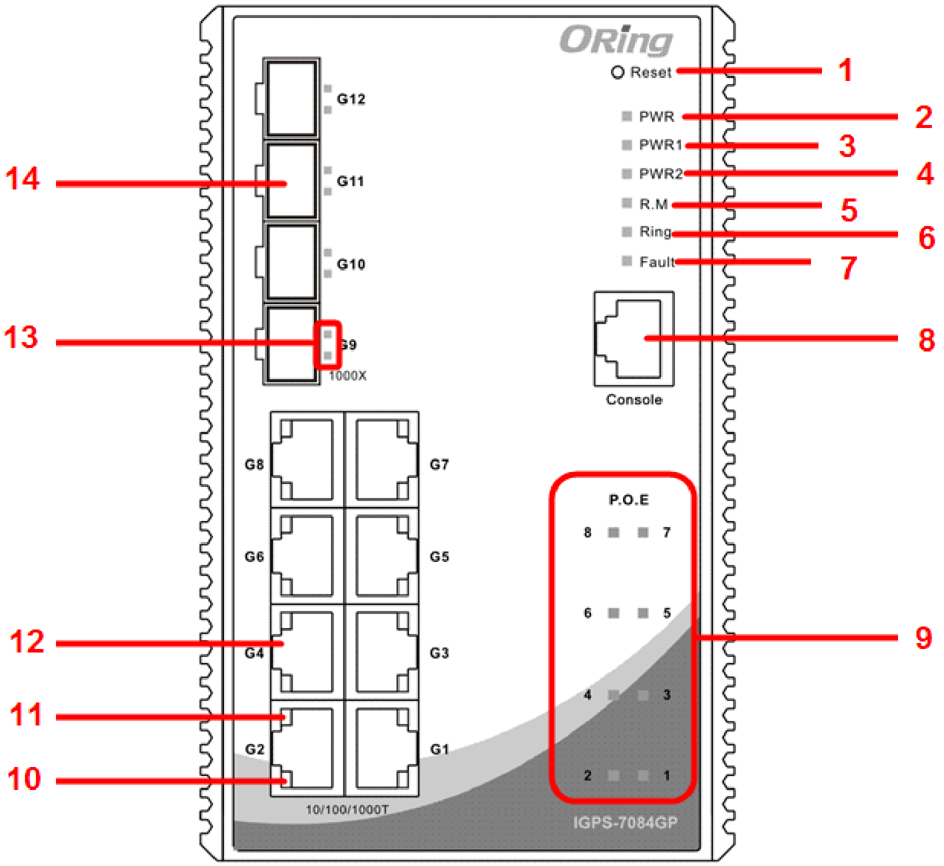
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IGPS-7084GP series.

Port	Description
SFP ports	4 1000BaseX on SFP port
Copper Port	8 1000 Base-T
Console	Use RS-232 with RJ-45 connecter to manage switch.

IGPS-7084GP



1. Reset button. Push the button 3 seconds for reset; 5 seconds for factory default.
2. LED for PWR. When the PWR UP, the green led will be light on
3. LED for PWR1
4. LED for PWR2
5. LED for R.M (Ring master). When the LED light on, it means that the switch is the ring

master of Ring.，LED for Ring.　When the led light on, it means the Ring is activated.

6. LED for Ring.　When the led light on, it means the O-Ring is activated.
7. LED for Fault. When the light on, it means Power failure or Port down/fail.
8. Console port (RJ-45)
9. LED for P.O.E Status.
10. LED for Ethernet ports link status.
11. LED for Ethernet ports speed status
12. 10/100/1000Base-T(X) ports
13. LED for SFP ports link status.
14. 1000 Base-X SFP

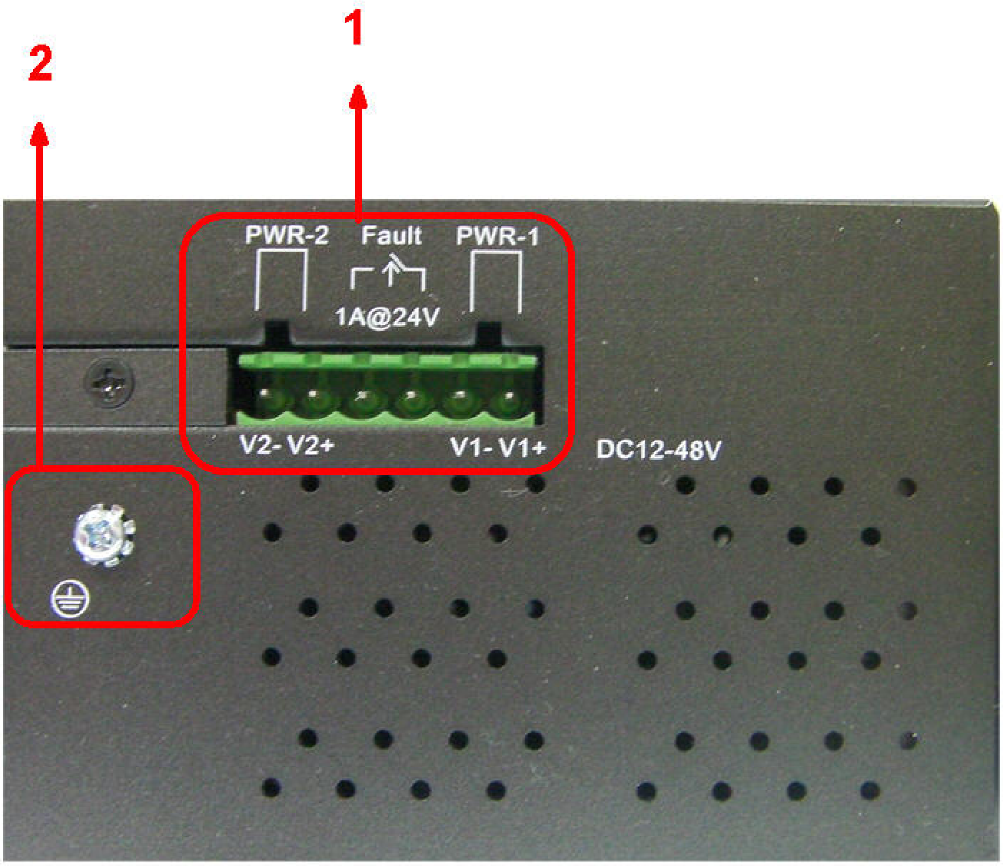
3.2 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power module up
PW1	Green	On	DC power module 1activated.
PW2	Green	On	DC Power module 2activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (lack of one link to build the ring.)
		Fast blinking	Ring work normally.
Fault	Amber	On	Fault relay.　Power failure or Port down/fail.
10/100Base-T(X) Fast Ethernet ports			
LNK	Green	On	Port link up.
ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
Gigabit Ethernet ports			
ACT	Amber	Blinking	Data transmitted.
LNK	Amber	Blinking	Port link up.
SFP			
LNK	Green	On	Port link up.
ACT	Green	On	Data transmitted.

3.3 Top view Panel

The bottom panel components of IGPS-7084GP Series are showed as below:

1. Terminal block includes: PWR1, PWR2 (12-48V DC)
2. Ground wire



.

Cables

4.1 Ethernet Cables

The IGPS-7084GP series switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

4.1.1 100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The IGPS-7084GP Series switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

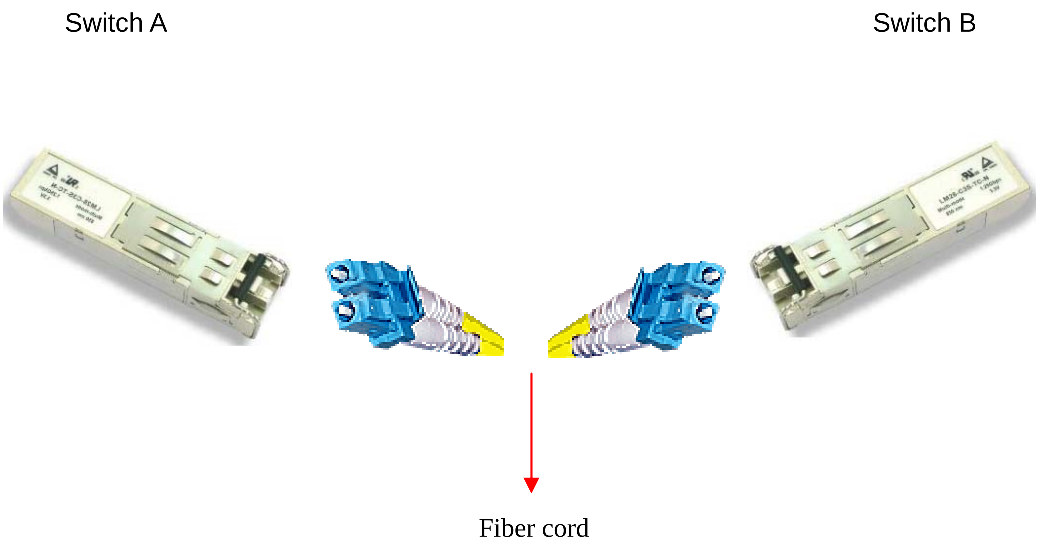
1000 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 SFP

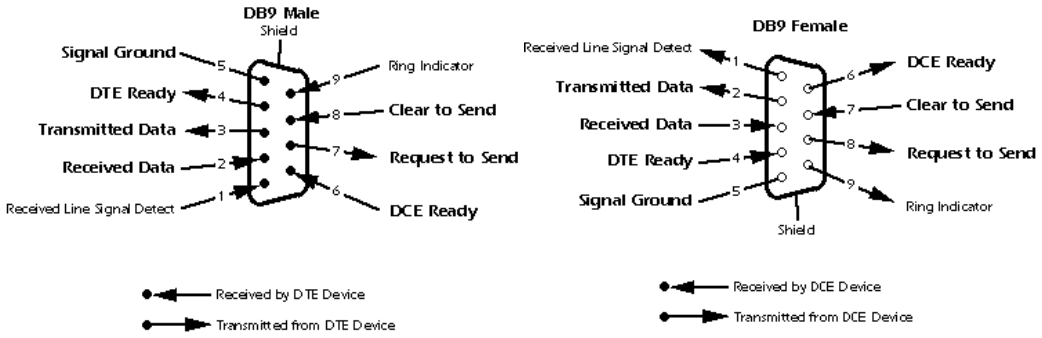
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 µm, 62.5/125 µm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



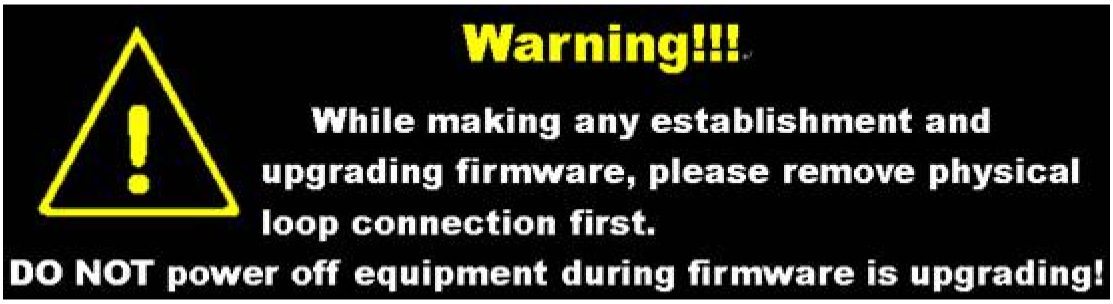
4.3 Console Cable

IGPS-7084GP Series switches can be management by console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



WEB Management



Warning!!!

While making any establishment and upgrading firmware, please remove physical loop connection first.

DO NOT power off equipment during firmware is upgrading!

5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

5.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

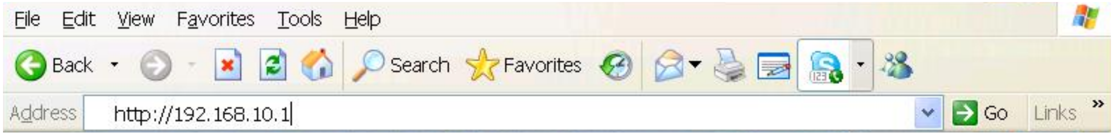
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

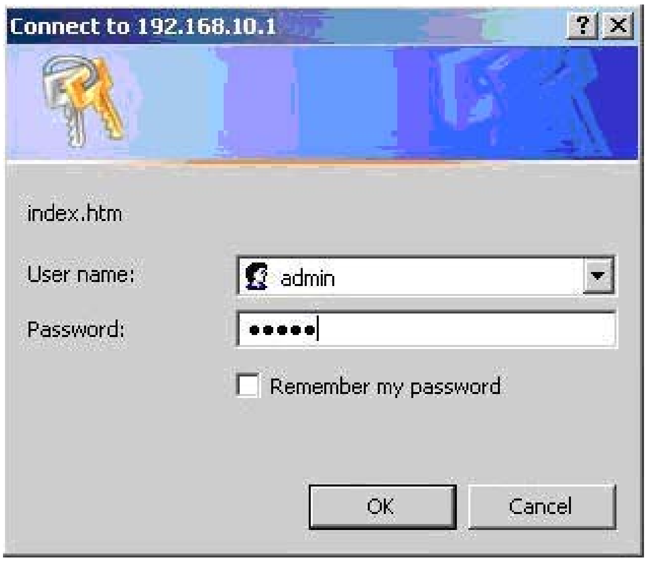
System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press "**Enter**".



Address http://192.168.10.1

3. The login screen appears.
4. Key in the username and password. The default username and password is "**admin**".
5. Click "**Enter**" or "**OK**" button, then the main interface of the Web-based management appears.



Connect to 192.168.10.1

index.htm

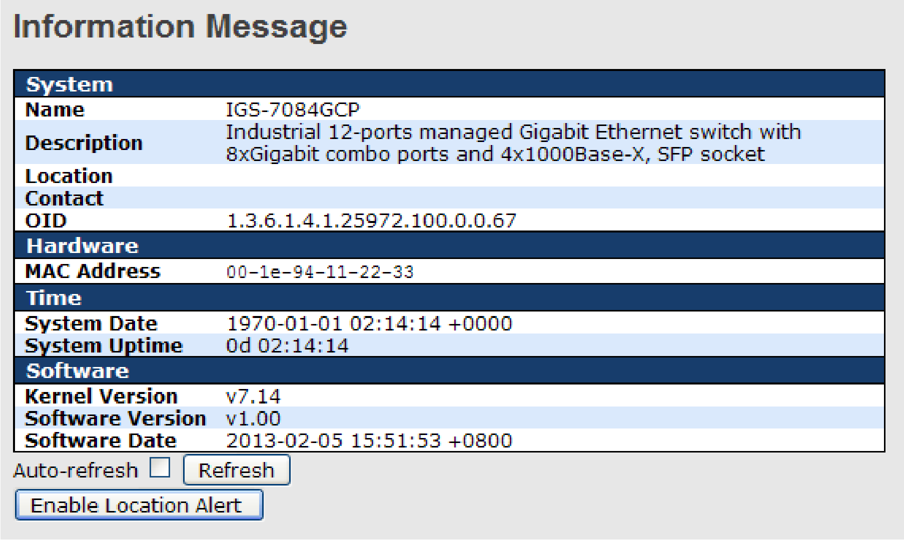
User name: admin

Password: •••••

□ Remember my password

Login screen

Main Interface



Information Message

System	
Name	IGS-7084GCP
Description	Industrial 12-ports managed Gigabit Ethernet switch with 8xGigabit combo ports and 4x1000Base-X, SFP socket
Location	
Contact	
OID	1.3.6.1.4.1.25972.100.0.0.67
Hardware	
MAC Address	00-1e-94-11-22-33
Time	
System Date	1970-01-01 02:14:14 +0000
System Uptime	0d 02:14:14
Software	
Kernel Version	v7.14
Software Version	v1.00
Software Date	2013-02-05 15:51:53 +0800

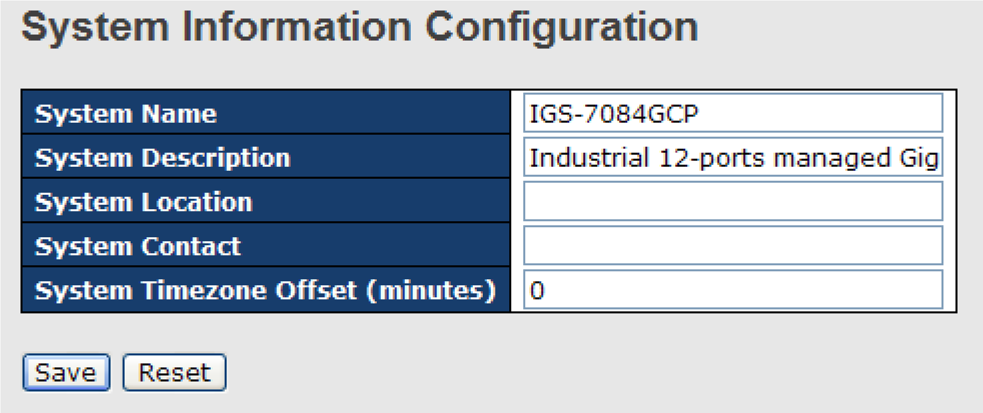
Auto-refresh □

Main interface

5.1.2 Basic Setting

5.1.2.1 System Information

The switch system information is provided here.



System Information Configuration

System Name	IGS-7084GCP
System Description	Industrial 12-ports managed Gig
System Location	
System Contact	
System Timezone Offset (minutes)	0

System Information interface

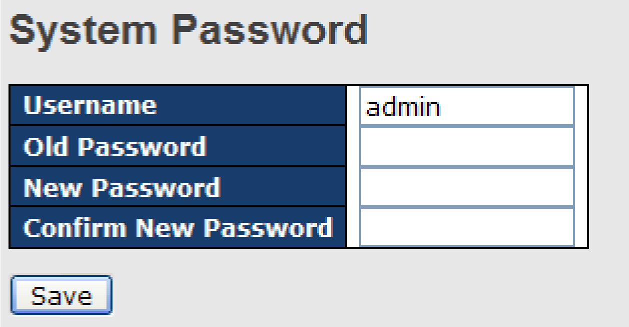
.

Label	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
Timezone Offset	Enter the name of contact person or organization Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2.2 Admin&Password

This page allows you to configure the system password required to access the web pages or log in from CLI.



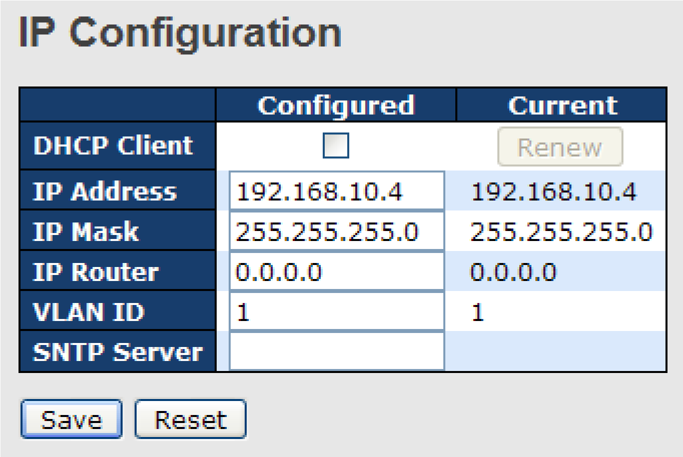
System Password

Username	admin
Old Password	
New Password	
Confirm New Password	

Label	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm password	Re-type the new password.
Save	Click to save changes.

5.1.2.3 IP Setting

Configure the switch-managed IP information on this page.



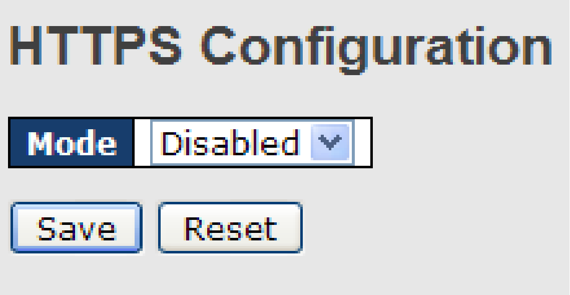
IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.10.4	192.168.10.4
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server		

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
SNTP Server	SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

5.1.2.4 HTTPS

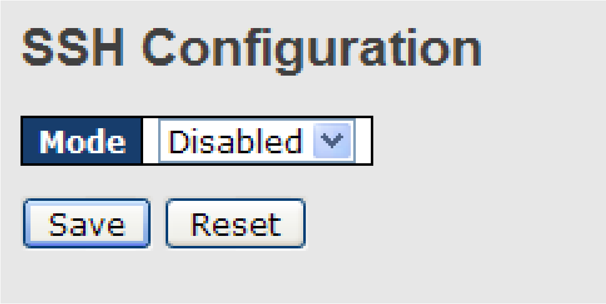


HTTPS Configuration

Mode: Disabled

Label	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2.5 SSH



SSH Configuration

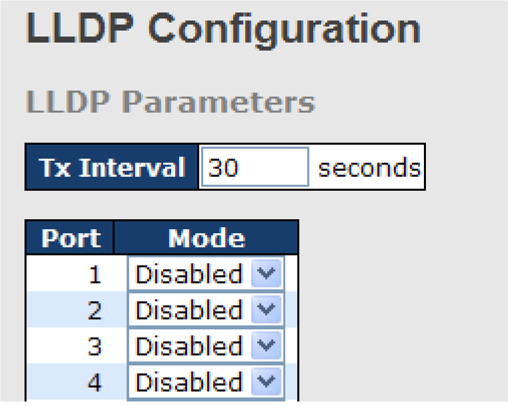
Mode: Disabled

Label	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2.6 LLDP

LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings.



LLDP Configuration

LLDP Parameters

Tx Interval: 30 seconds

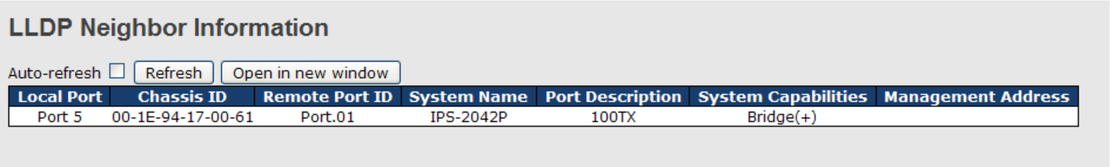
Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled

Label	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode.

	Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:



LLDP Neighbor Information

Auto-refresh □ Refresh Open in new window

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 5	00-1E-94-17-00-61	Port.01	IPS-2042P	100TX	Bridge(+)	

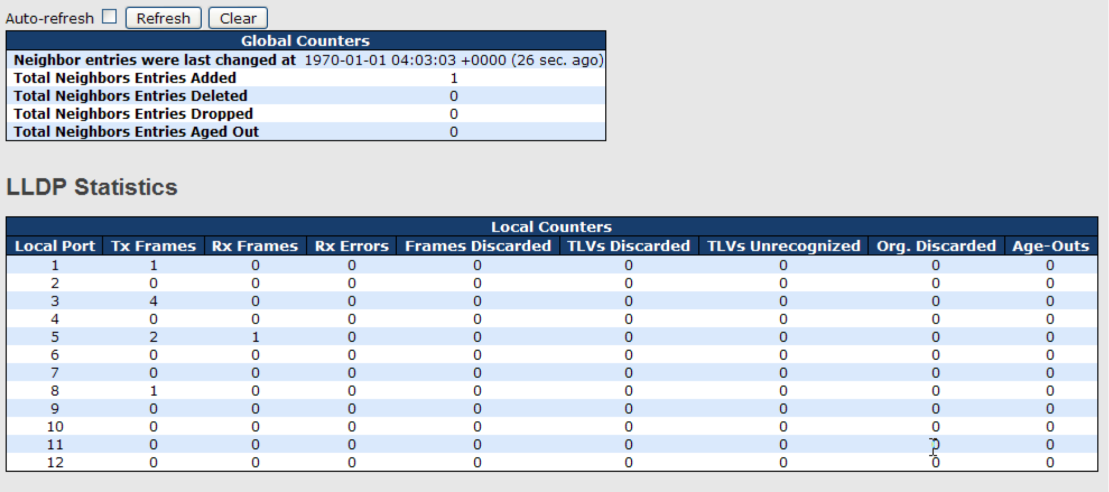
Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilites	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone

	7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.



Global Counters	
Neighbor entries were last changed at	1970-01-01 04:03:03 +0000 (26 sec. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	4	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	2	1	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	1	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

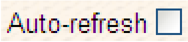
Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time elaP.S.E.d since last change was detected.
Total Neighbors	Shows the number of new entries added since switch reboot.

Entries Added	
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

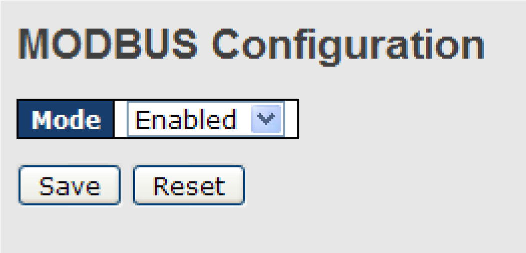
Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Refresh	Click to refresh the page immediately.
Clear	Clears the local counters. All counters (including global counters) are cleared upon reboot.

 Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.2.7 Modbus TCP

Support Modbus TCP .(About Modbus please reference http://www.modbus.org/)



MODBUS Configuration

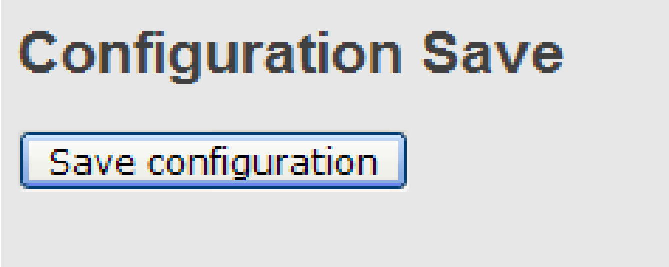
Mode: Enabled

The following table describes the labels in this screen.

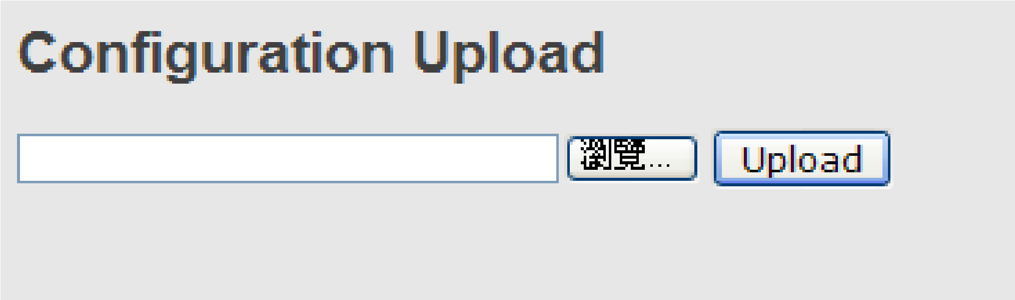
Label	Description
Mode	Enable or Disalble Modbus TCP function

5.1.2.8 Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:



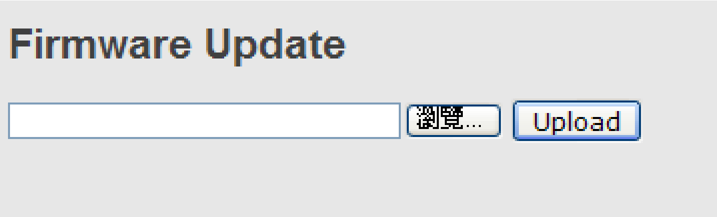
Configuration Save



Configuration Upload

5.1.2.9 Firmware Update

This page facilitates an update of the firmware controlling the stack. switch.

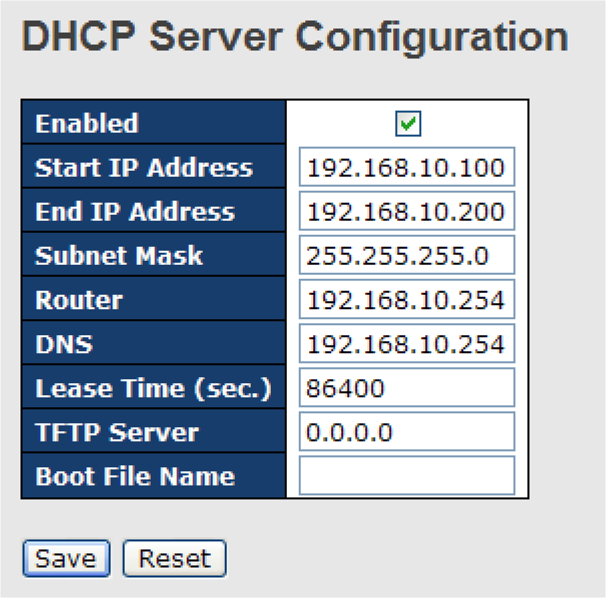


Firmware Update

5.1.3 DHCP Server

5.1.3.1 Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

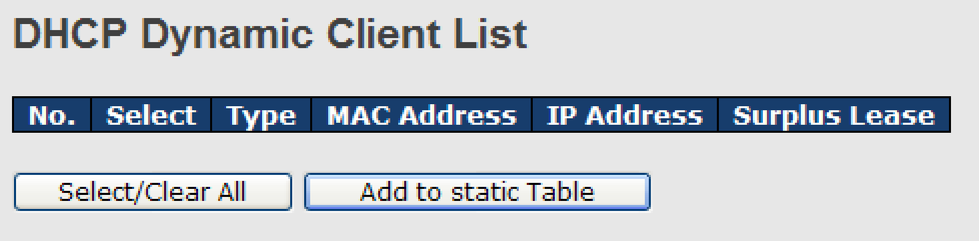


DHCP Server Configuration

Enabled	☑
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Router	192.168.10.254
DNS	192.168.10.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

5.1.3.2 DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.

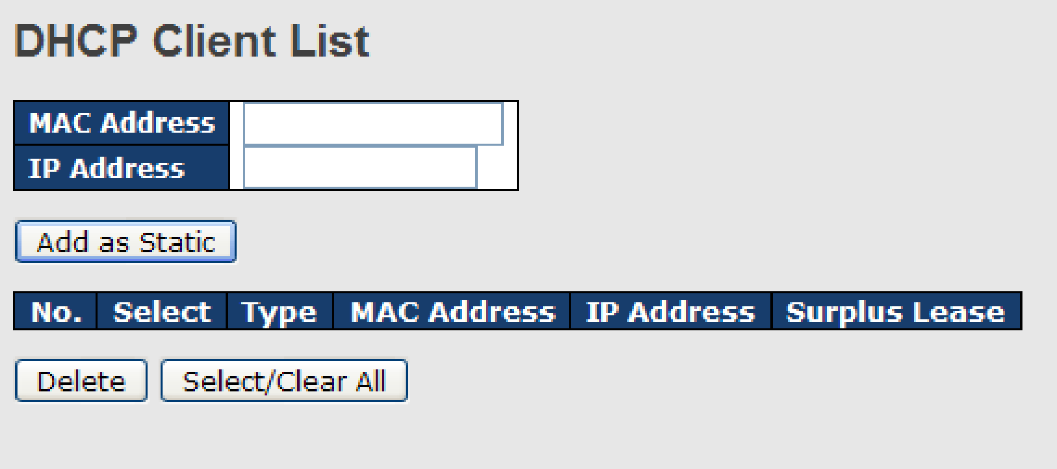


DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease

5.1.3.3 DHCP Client List

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.



DHCP Client List

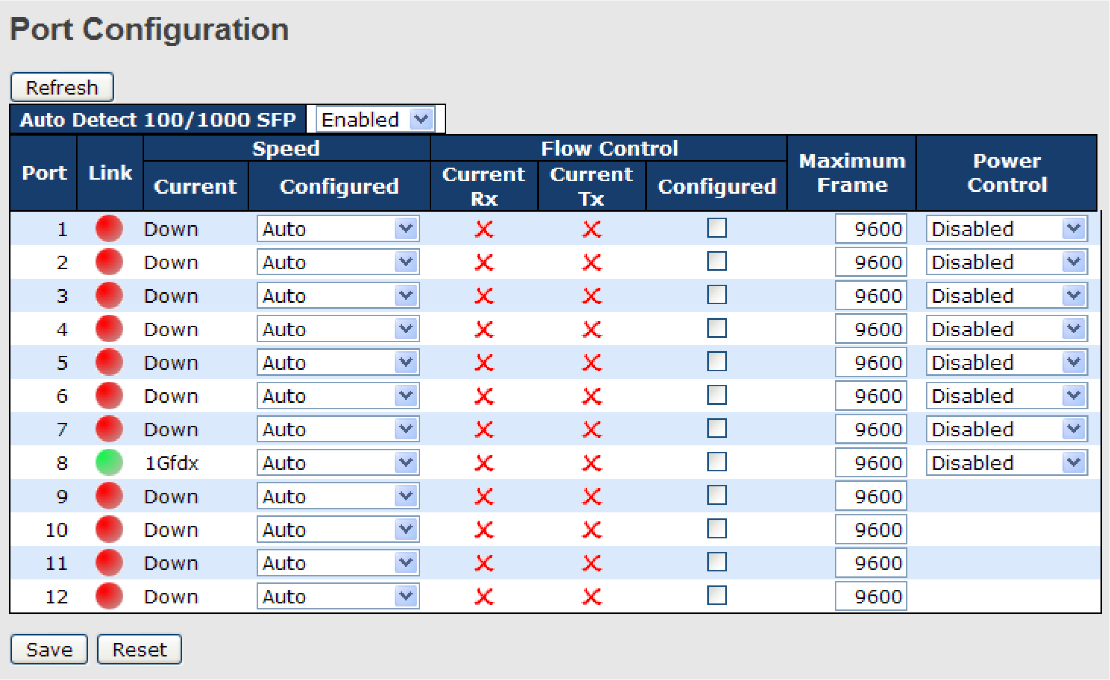
MAC Address	
IP Address	

No.	Select	Type	MAC Address	IP Address	Surplus Lease

5.1.4 Port Setting

5.1.4.1 Port Control

This page displays current port configurations. Ports can also be configured here.



Port Configuration

Refresh

Auto Detect 100/1000 SFP: Enabled

Port	Link	Speed		Flow Control			Maximum Frame	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
1	🔴	Down	Auto	✗	✗	□	9600	Disabled
2	🔴	Down	Auto	✗	✗	□	9600	Disabled
3	🔴	Down	Auto	✗	✗	□	9600	Disabled
4	🔴	Down	Auto	✗	✗	□	9600	Disabled
5	🔴	Down	Auto	✗	✗	□	9600	Disabled
6	🔴	Down	Auto	✗	✗	□	9600	Disabled
7	🔴	Down	Auto	✗	✗	□	9600	Disabled
8	🟢	1Gfdx	Auto	✗	✗	□	9600	Disabled
9	🔴	Down	Auto	✗	✗	□	9600	
10	🔴	Down	Auto	✗	✗	□	9600	
11	🔴	Down	Auto	✗	✗	□	9600	
12	🔴	Down	Auto	✗	✗	□	9600	

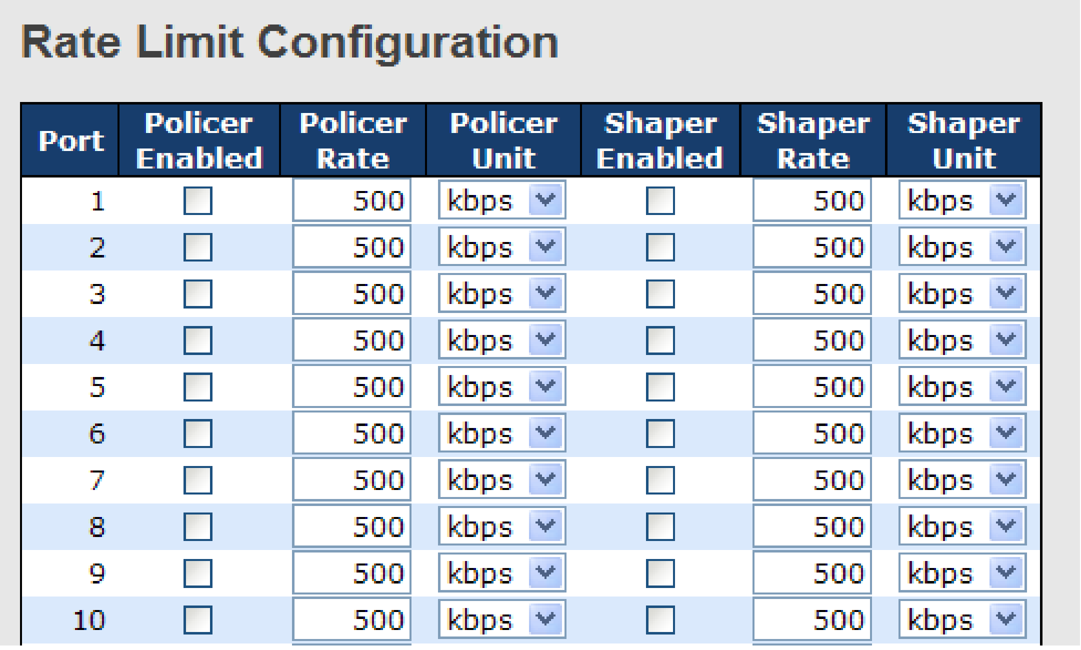
Save Reset

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed that is compatible with a link partner. Disabled disables the switch port operation.
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is

	related to the setting for Configured Link Speed.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collsion Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart backoff algorithm after 16 collisions.
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled.
Total Power Usage	Total power usage in board, measured in percent.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

5.1.4.2 Rate Limit

Configure the switch port rate limit for Policers and Shapers on this page.



Rate Limit Configuration

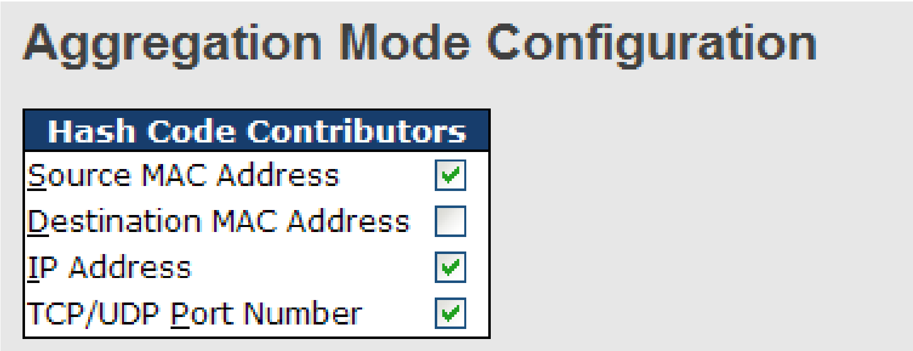
Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps
9	□	500	kbps	□	500	kbps
10	□	500	kbps	□	500	kbps

Label	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.4.3 Port Trunk

5.1.4.3.1 Trunk Configuration

This page is used to configure the Aggregation hash mode and the aggregation group.

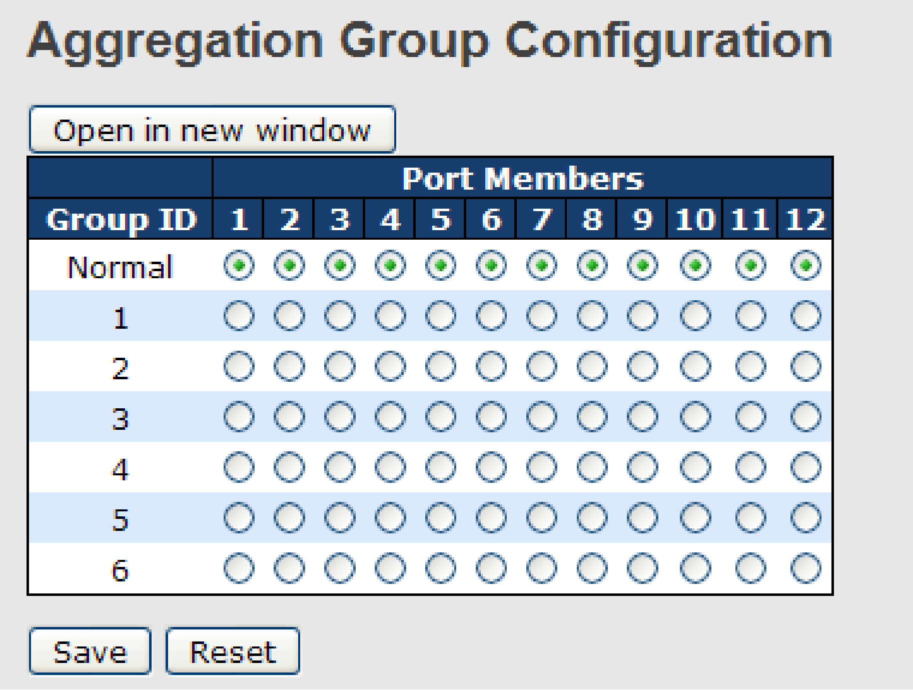


Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the

	Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.



Aggregation Group Configuration

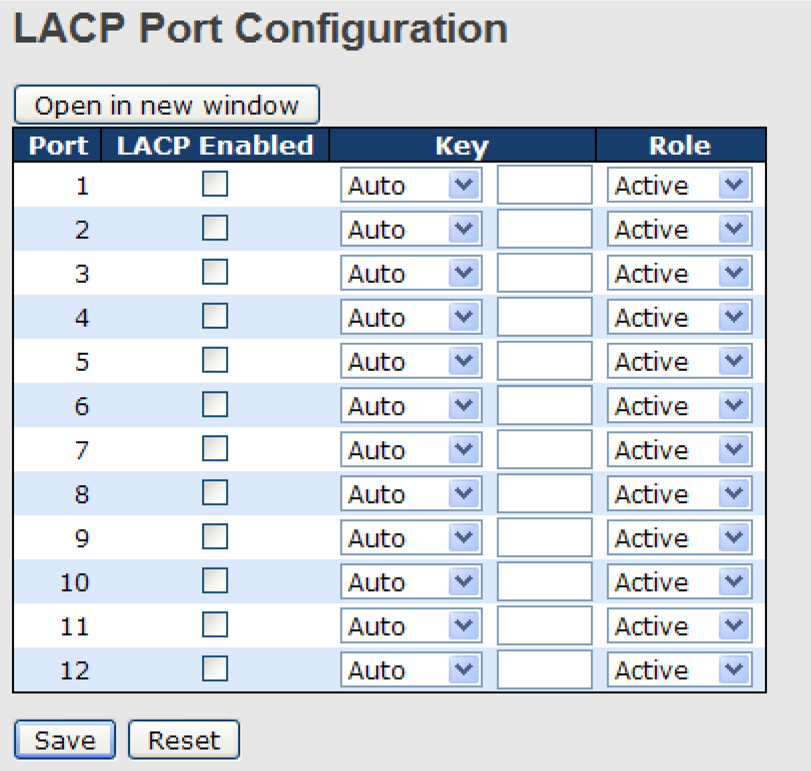
	Port Members											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12
Normal	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○

Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong

	to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

5.1.4.3.2 LACP Port Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.



LACP Port Configuration

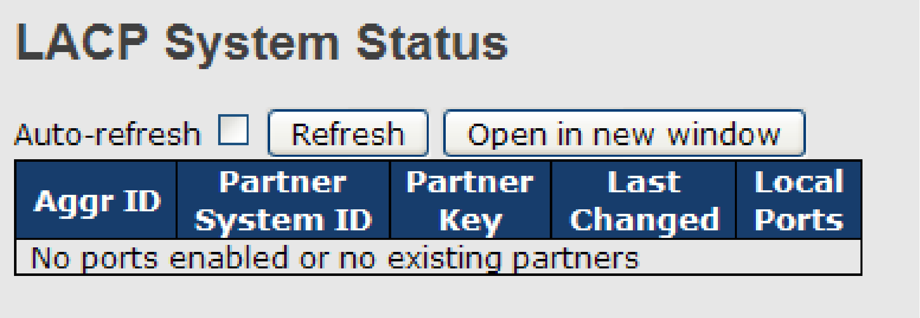
Port	LACP Enabled	Key		Role
1	☐	Auto		Active
2	☐	Auto		Active
3	☐	Auto		Active
4	☐	Auto		Active
5	☐	Auto		Active
6	☐	Auto		Active
7	☐	Auto		Active
8	☐	Auto		Active
9	☐	Auto		Active
10	☐	Auto		Active
11	☐	Auto		Active
12	☐	Auto		Active

Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value

	can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.4.3.3 LACP System Status

This page provides a status overview for all LACP instances.



LACP System Status

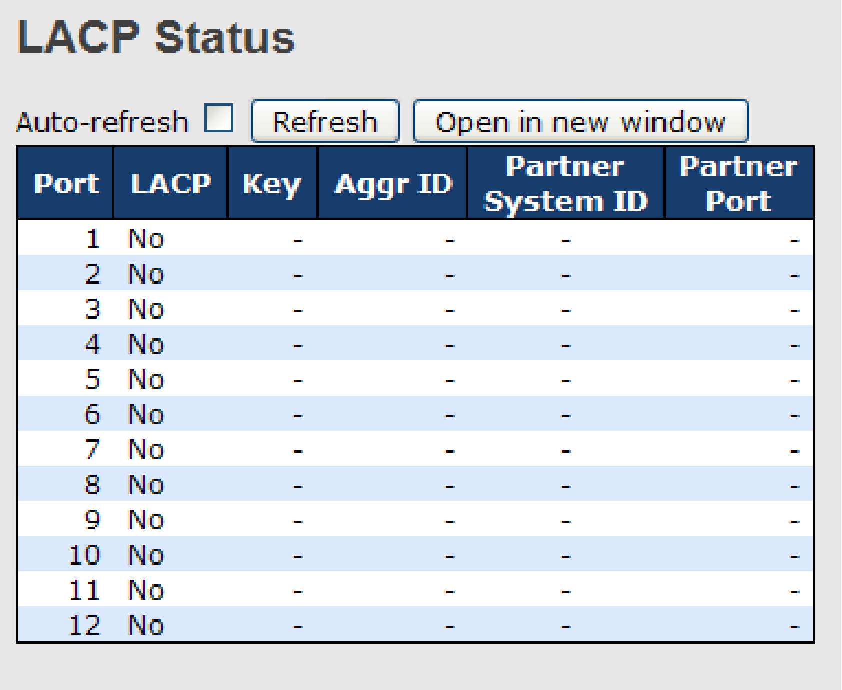
Auto-refresh □ Refresh Open in new window

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Last Channged	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.4.3.4 LACP Status

This page provides a status overview for LACP status for all ports.



LACP Status

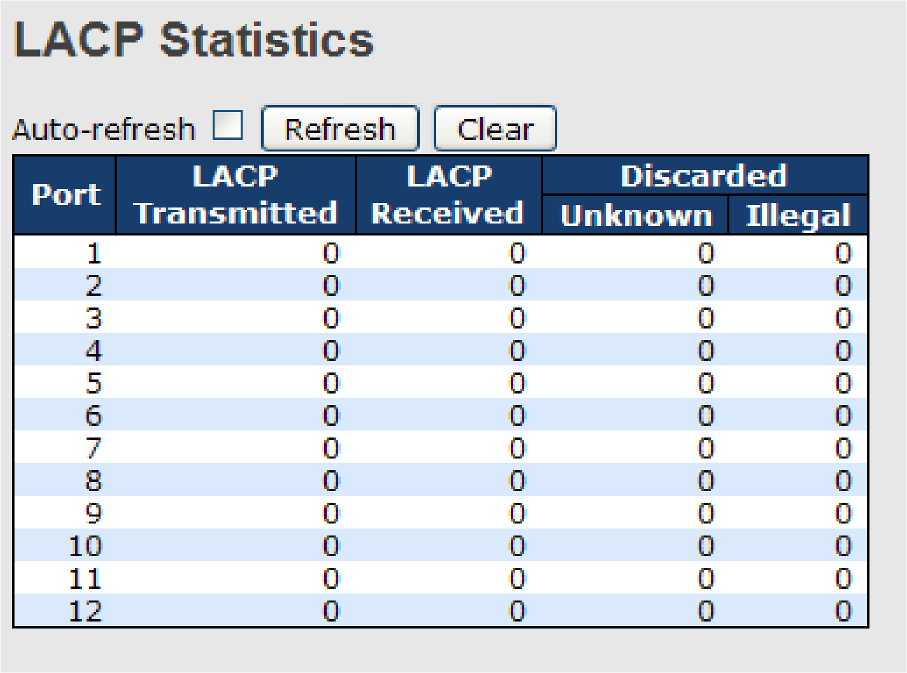
Auto-refresh □ Refresh Open in new window

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-

Label	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.4.3.5 LACP Statistics

This page provides an overview for LACP statistics for all ports.



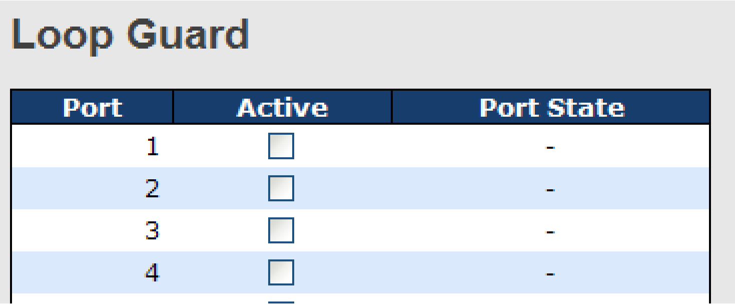
LACP Statistics

Port	LACP Transmitted	LACP Received	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Label	Description
Port	The switch port number
LACP Transmitted	Shows how many LACP frames have been sent from each port
LACP Received	Shows how many LACP frames have been received at each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.
Clear	Clears the counters for all ports

5.1.4.4 Loop Gourd

This feature prevents the loop attack,When the port receives loop packet. This port will auto disable , prevent the "loop attack" affect other network devices



Loop Guard

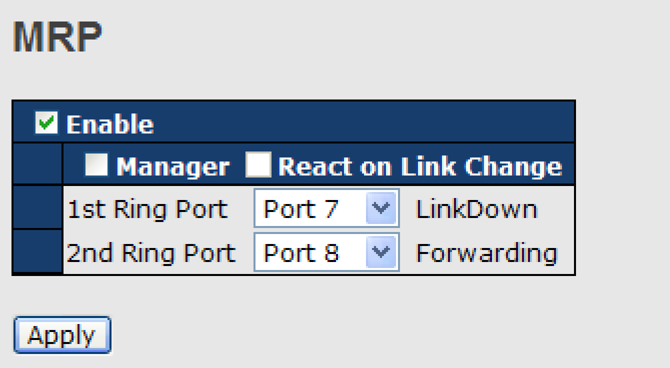
Port	Active	Port State
1	□	-
2	□	-
3	□	-
4	□	-

Label	Description
Active	Loop Guard Enable or Disable
Port Status	Port work status.

5.1.5 Redundancy

5.1.5.1 MRP

MRP (Media Redundancy Protocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).



MRP

☑ Enable

□ Manager □ React on Link Change

1st Ring Port: Port 7 — LinkDown

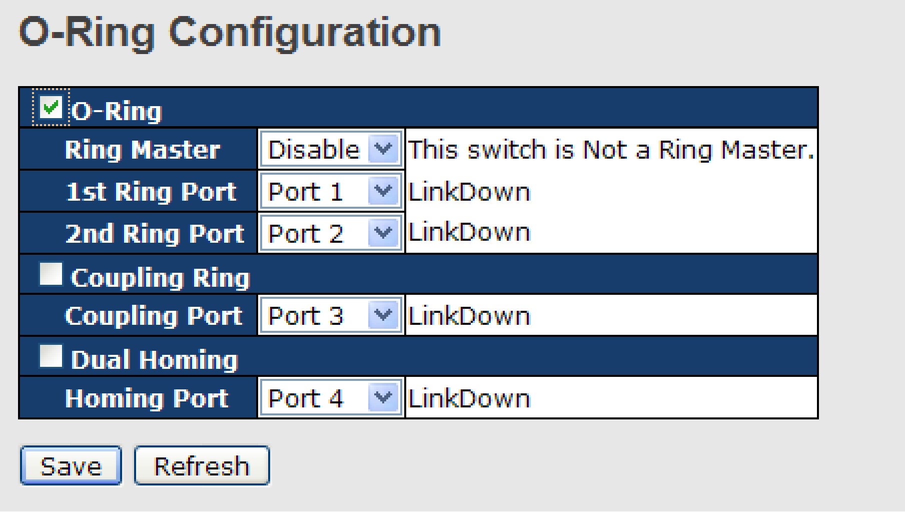
2nd Ring Port: Port 8 — Forwarding

Label	**Description**
Enable	Enabling the MRP function
Manager	MRP Master , every one MRP topology , need setting one device to Manager.(one MRP topology only can setting one device to Manager, if user setting two or more switch to Manager, this MRP topology will fail.)

React on Link Change (Advanced mode)	Faster mode, if user enable this function , MRP Topology will more faster convergence, this function only can setting in MRP Manager Switch.
1st Ring Port	Choosing the port which connect to the MRP ring
2nd Ring Port	Choosing the port which connect to the MRP ring

5.1.5.2 O-Ring

Ring is the most powerful Ring in the world. The recovery time of Ring is less than 10 ms. It can reduce unexpected damage caused by network topology change. Ring Supports 3 Ring topology: Ring, Coupling Ring and Dual Homing.



O-Ring Configuration

☑ O-Ring		
Ring Master	Disable	This switch is Not a Ring Master.
1st Ring Port	Port 1	LinkDown
2nd Ring Port	Port 2	LinkDown
□ Coupling Ring		
Coupling Port	Port 3	LinkDown
□ Dual Homing		
Homing Port	Port 4	LinkDown

Ring interface

The following table describes the labels in this screen.

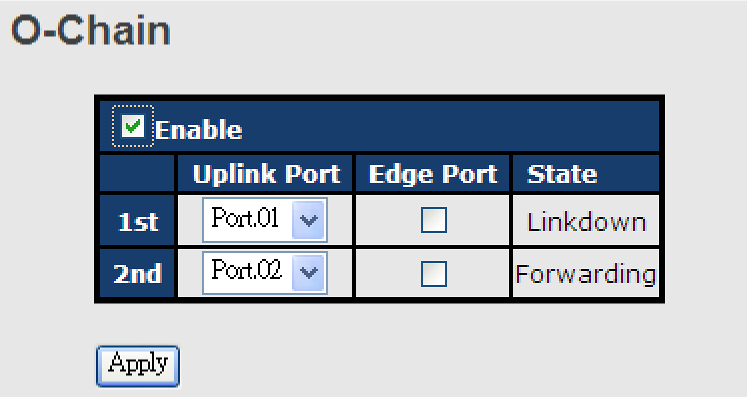
Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.

Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to set the configurations.

Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

5.1.5.3 O-Chain

O-Chain is the revolutionary network redundancy technology that provides the add-on network redundancy topology for any backbone network, providing ease-of-use while maximizing fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in one set of network redundancy topologies O-Chain allows multiple redundant network rings of different redundancy protocols to join and function together as a larger and more robust compound network topology, i.e. the creation of multiple redundant networks beyond the limitations of current redundant ring technology.

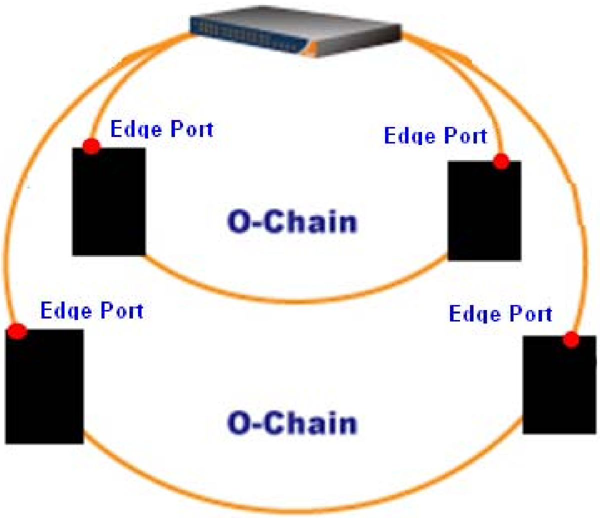


O-Chain

☑ Enable

	Uplink Port	Edge Port	State
1st	Port.01	□	Linkdown
2nd	Port.02	□	Forwarding

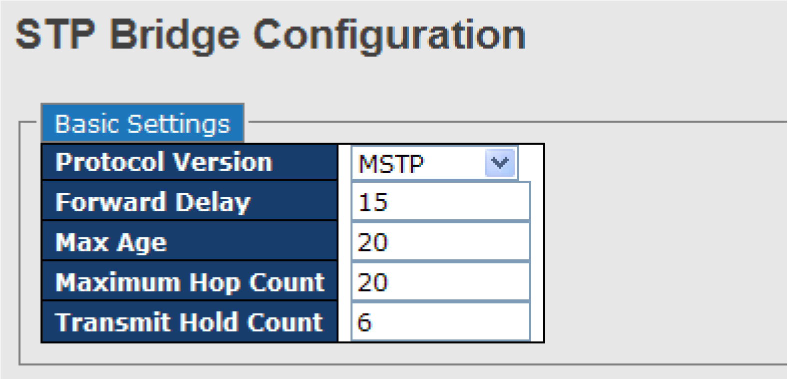
Label	Description
Enable	Enabling the O-Chain function
1st Ring Port	Choosing the port which connect to the ring
2nd Ring Port	Choosing the port which connect to the ring
Edge Port	In the O-Chain application, the head and tail of two Switch Port, must start the Edge,MAC smaller Switch, Edge port will be the backup and RM LED Light.



5.1.5.4 MSTP

Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.



STP Bridge Configuration

Basic Settings

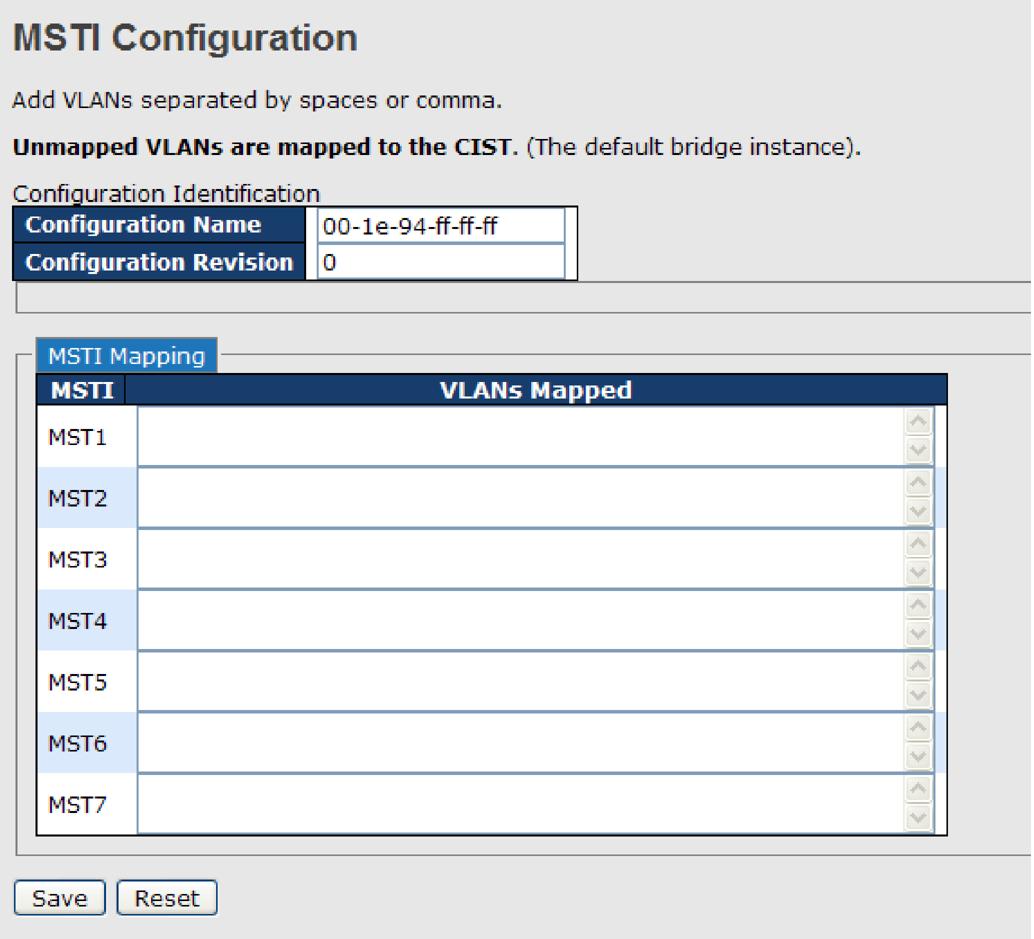
Protocol Version	MSTP
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remainingHops for MSTI

	information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-1e-94-ff-ff-ff
Configuration Revision	0

MSTI Mapping

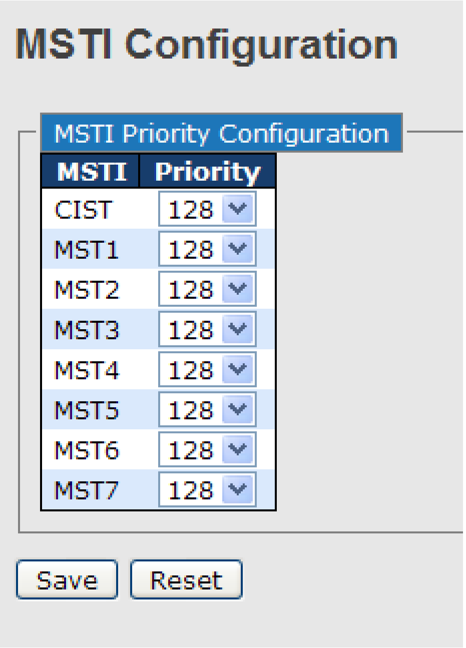
MSTI	VLANs Mapped
MST1	
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	

Label	Description

Configuration Name	The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANS Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



MSTI Configuration

MSTI Priority Configuration

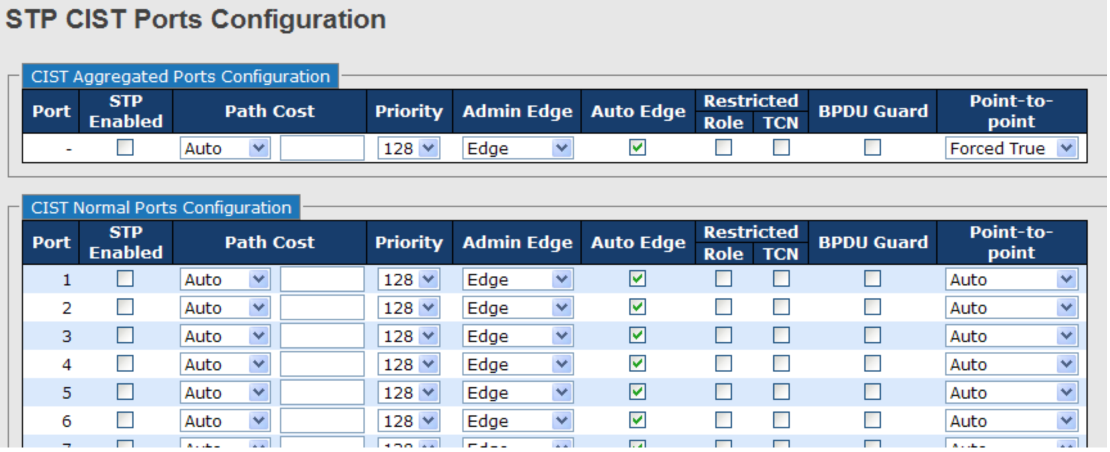
MSTI	Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

Label	Description

MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.This page contains settings for physical and aggregated ports. The aggregation settings are stack global.



STP CIST Ports Configuration

CIST Aggregated Ports Configuration

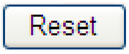
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☐	Auto		128	Edge	☑	☐	☐	☐	Forced True

CIST Normal Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
1	☐	Auto		128	Edge	☑	☐	☐	☐	Auto
2	☐	Auto		128	Edge	☑	☐	☐	☐	Auto
3	☐	Auto		128	Edge	☑	☐	☐	☐	Auto
4	☐	Auto		128	Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Edge	☑	☐	☐	☐	Auto
6	☐	Auto		128	Edge	☑	☐	☐	☐	Auto

Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost

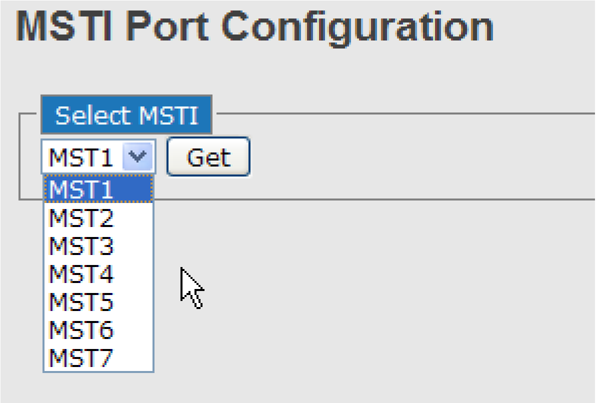
	ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
OpenEdge(setate flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
AdminEdge	Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.

 Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated seperately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

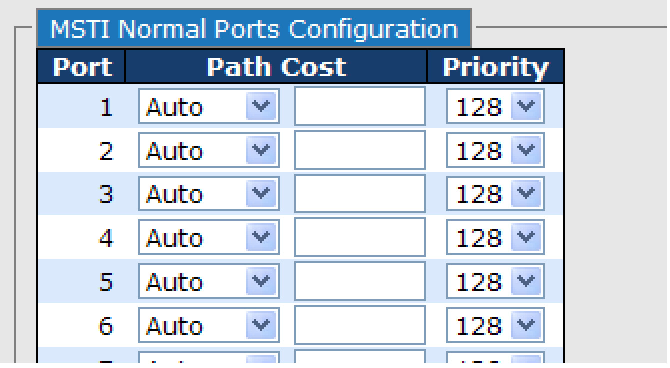
This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.



MSTI Port Configuration

Select MSTI

MST1 Get



MSTI Normal Ports Configuration

Port	Path Cost		Priority
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128

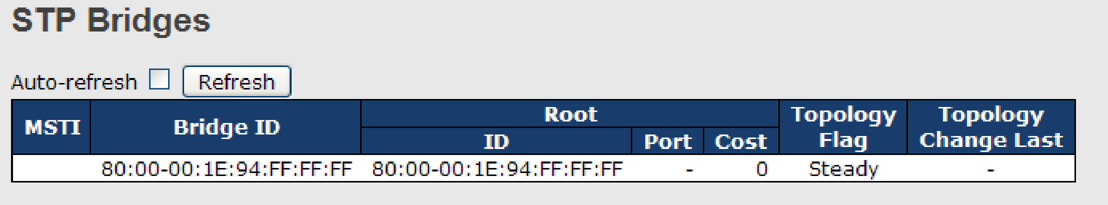
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when

	establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

STP Bridges

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:



STP Bridges

Auto-refresh □ Refresh

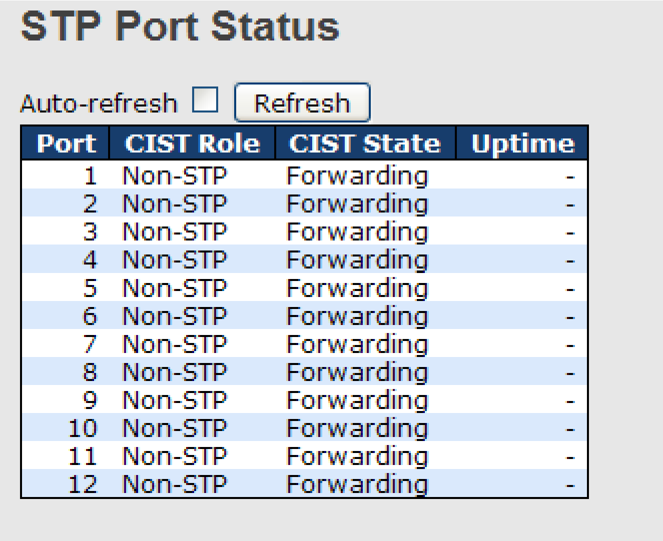
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
	80:00-00:1E:94:FF:FF:FF	80:00-00:1E:94:FF:FF:FF	-	0	Steady	-

Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Click to refresh the page immediately.

Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.



STP Port Status

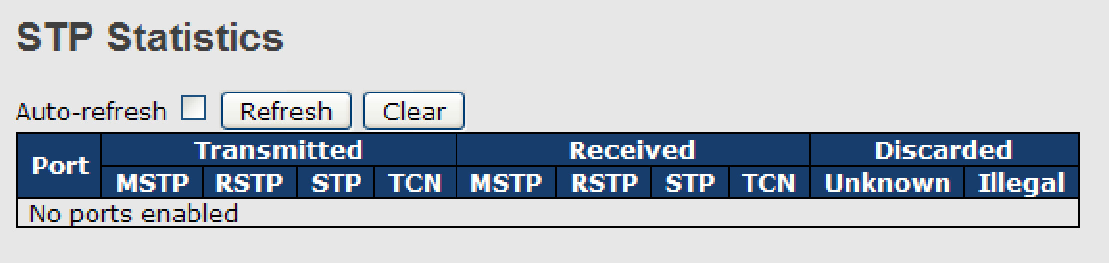
Auto-refresh □ Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-

Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was last initialized.
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.



STP Statistics

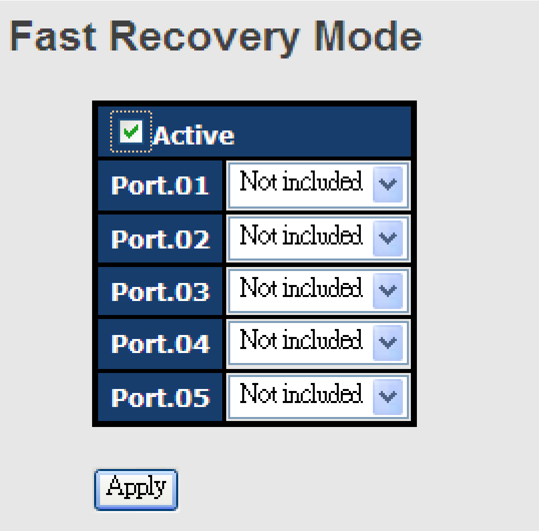
Auto-refresh □ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.5.5 Fast Recovery mode

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The TES-250-M12 with its fast recovery mode will provide redundant links. Fast Recovery mode supports 5 priorities, only the first priority will be the act port, the other ports configured with other priority will be the backup ports.



Fast Recovery Mode

☑ Active	
Port.01	Not included
Port.02	Not included
Port.03	Not included
Port.04	Not included
Port.05	Not included

Fast Recovery Mode interface

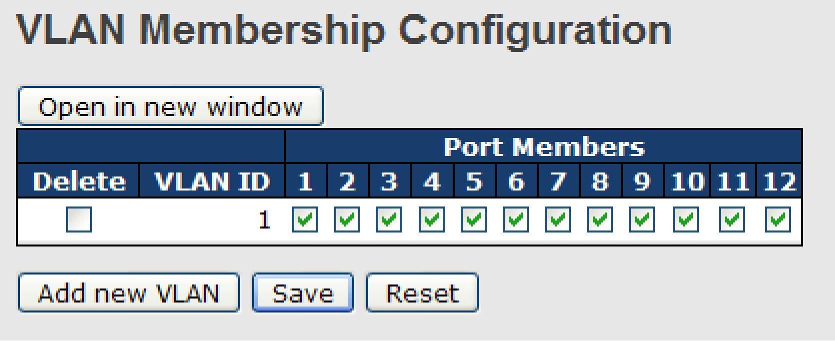
The following table describes the labels in this screen.

Label	Description
Active	Activate the fast recovery mode.
port	Port can be configured as 5 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest.
Apply	Click "**Apply**" to activate the configurations.

5.1.6 VLAN

5.1.6.1 VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



VLAN Membership Configuration

		Port Members											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

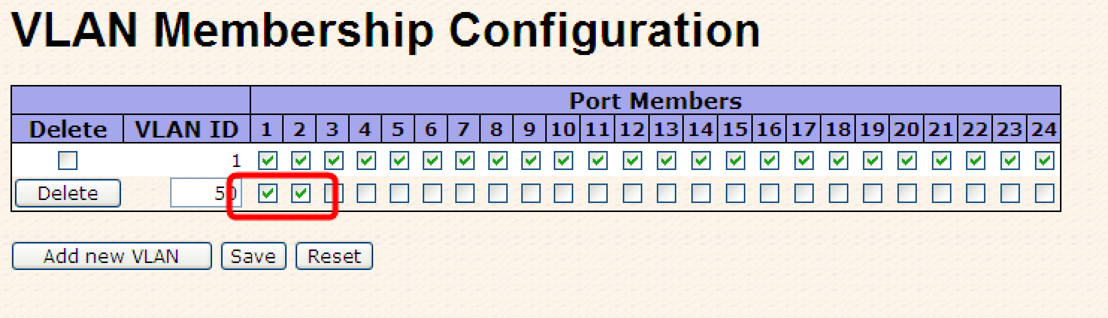
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add New VLAN to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The Delete button can be used to undo the addition of new VLANs.

Example:

Portbased VLAN Setting

(For ingress port)

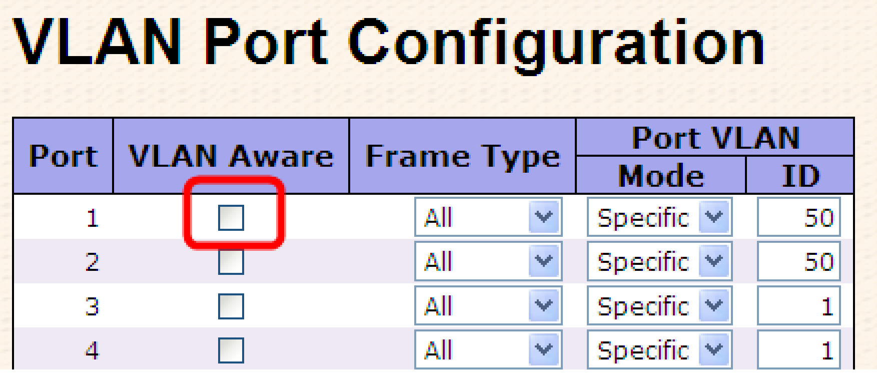
1. VLAN Membership Configuration setting port 1 & VID=50



VLAN Membership Configuration

		Port Members																							
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	50	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

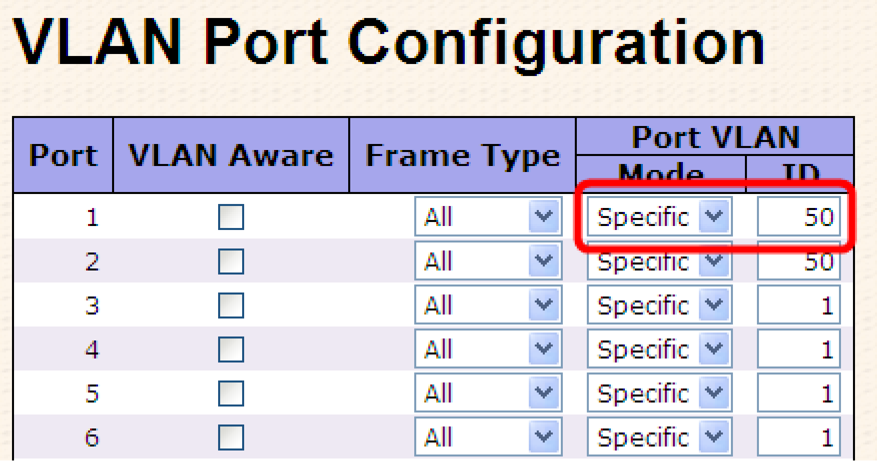
2. VLAN Port 1 Configuration-->Disable VLAN Aware



VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	50
3	□	All	Specific	1
4	□	All	Specific	1

3. VLAN Port 1 Configuration-->Mode=specific,ID=50

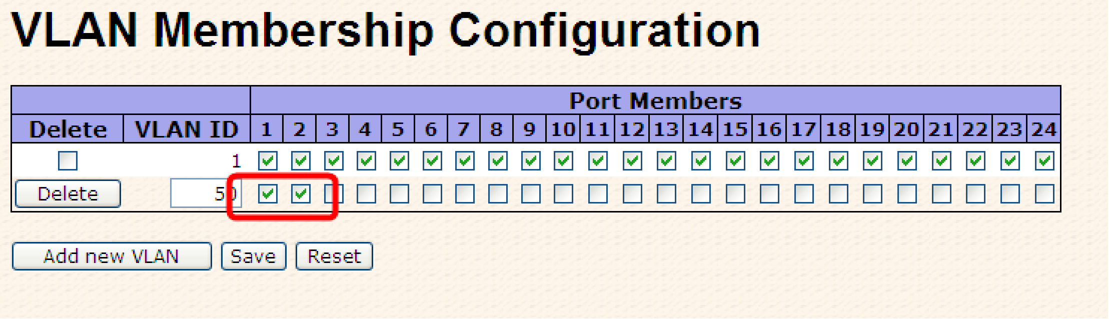


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	50
3	□	All	Specific	1
4	□	All	Specific	1
5	□	All	Specific	1
6	□	All	Specific	1

(For egress port)

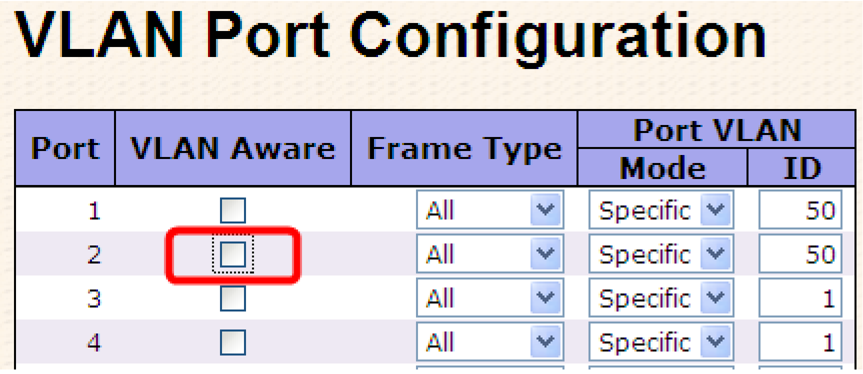
1. VLAN Membership Configuration setting port 2 & VID=50



VLAN Membership Configuration

Delete	VLAN ID	Port Members																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	50	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

2. VLAN Port 2 Configuration-->don't care VLAN Aware

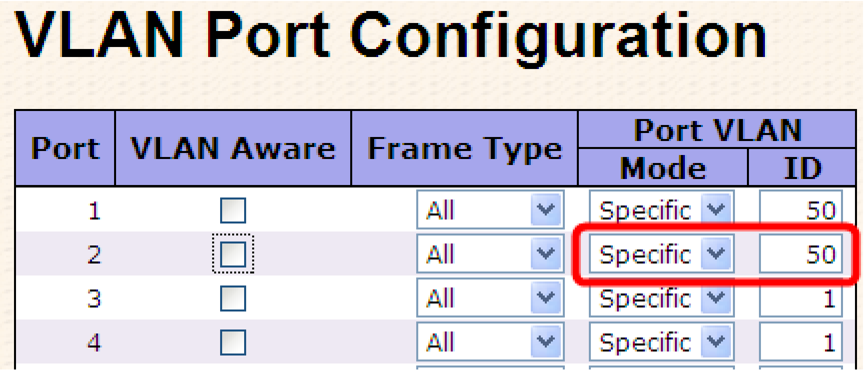


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	50
3	□	All	Specific	1
4	□	All	Specific	1

3. VLAN Port 2 Configuration-->Mode=specific,ID=50

(any packet can enter egress port)



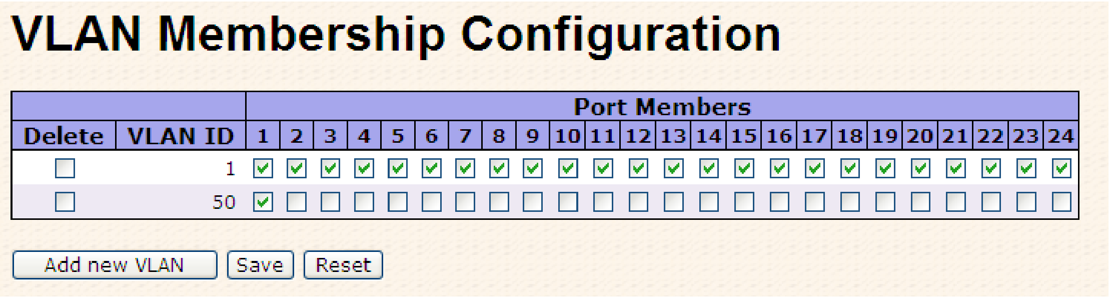
VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	50
3	□	All	Specific	1
4	□	All	Specific	1

802.1Q Access port Setting

(For ingress port)

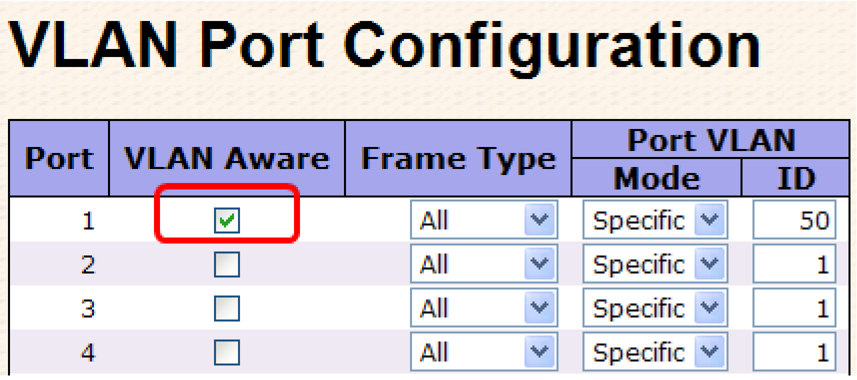
1. VLAN Membership Configuration setting port & VID=50



VLAN Membership Configuration

		Port Members																							
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	50	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

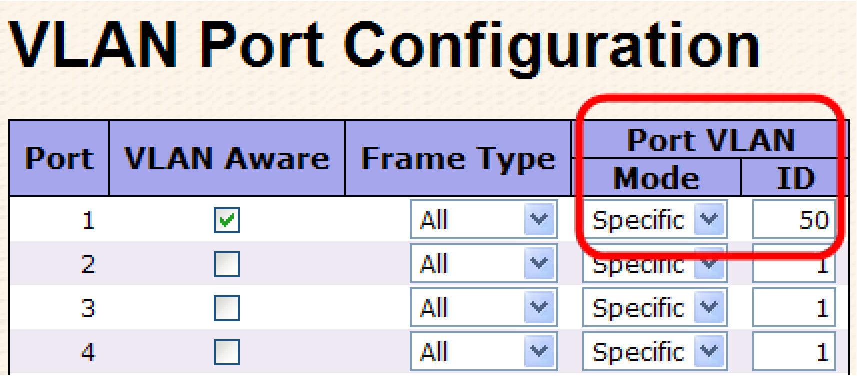
2. VLAN Port Configuration-->Enable VLAN Aware



VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	☑	All	Specific	50
2	□	All	Specific	1
3	□	All	Specific	1
4	□	All	Specific	1

3. VLAN Port Configuration-->Mode=specific,ID=50

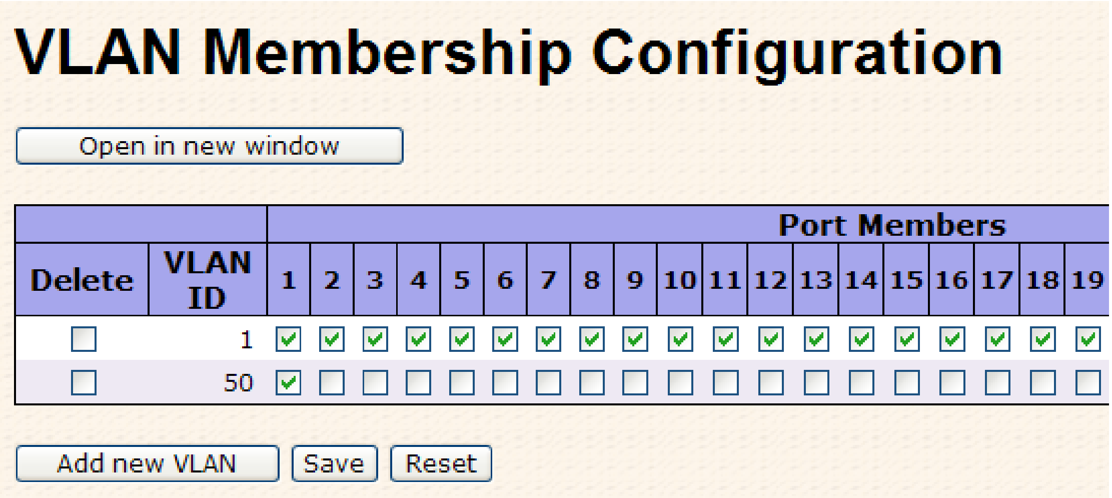


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	☑	All	Specific	50
2	□	All	Specific	1
3	□	All	Specific	1
4	□	All	Specific	1

(For egress port)

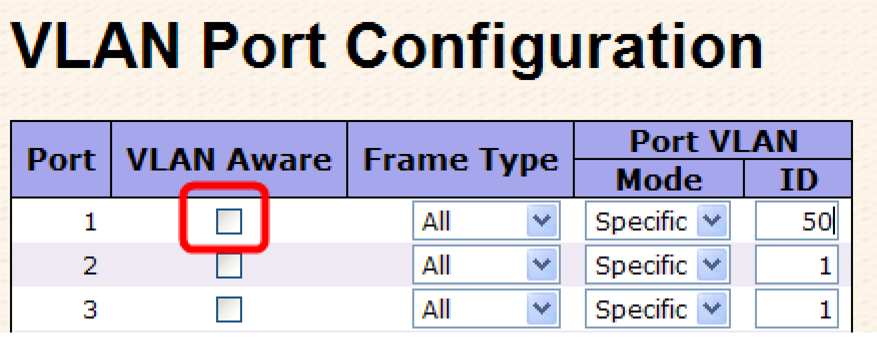
1. VLAN Membership Configuration setting port & VID=50



VLAN Membership Configuration

		Port Members																		
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	50	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

2. VLAN Port Configuration-->Disable VLAN Aware

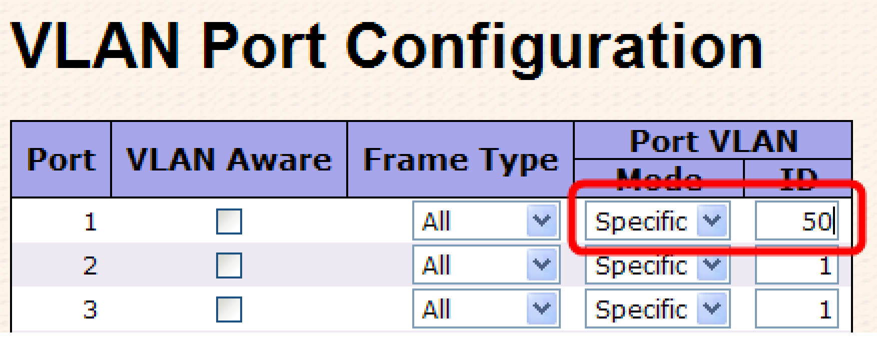


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	1
3	□	All	Specific	1

3. VLAN Port Configuration-->Mode=specific,ID=50

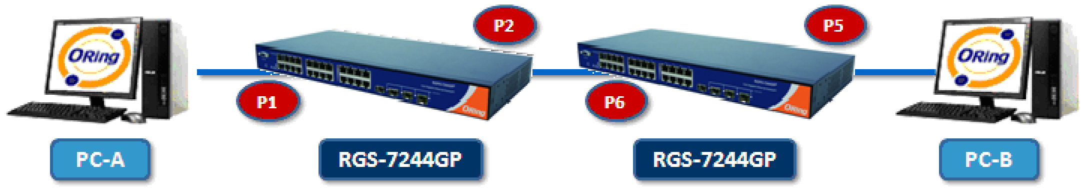
(untagged & tag=50 packet can enter egress port)



VLAN Port Configuration

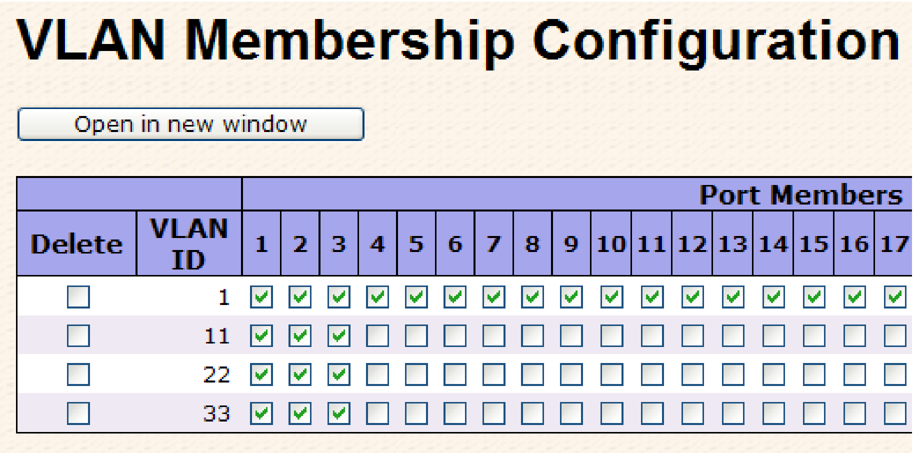
Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	□	All	Specific	1
3	□	All	Specific	1

802.1Q Trunk port setting (multi-tag)



(For ingress port)

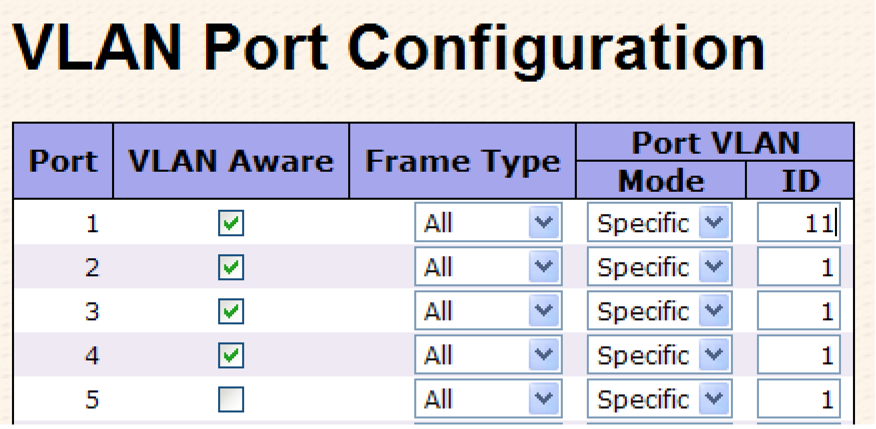
1. VLAN Membership Configuration setting port & VID=11,22,33



VLAN Membership Configuration

		Port Members																
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	11	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	22	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	33	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□

2. VLAN Port Configuration-->Enable VLAN Aware

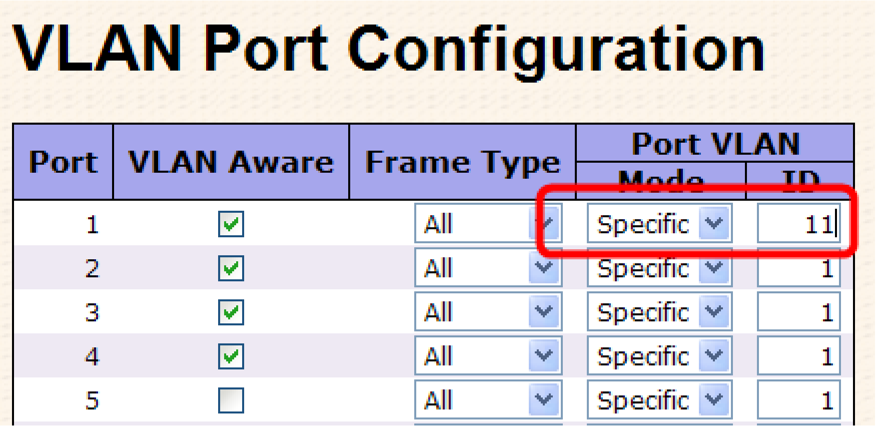


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	Port VLAN ID
1	☑	All	Specific	11
2	☑	All	Specific	1
3	☑	All	Specific	1
4	☑	All	Specific	1
5	□	All	Specific	1

3. VLAN Port Configuration-->Mode=specific,ID=11

(when enterring packet is untagged frame, added tag = 11 ,When entering the tagged frame, only VID = 11,22,33 three kinds of packets can pass)

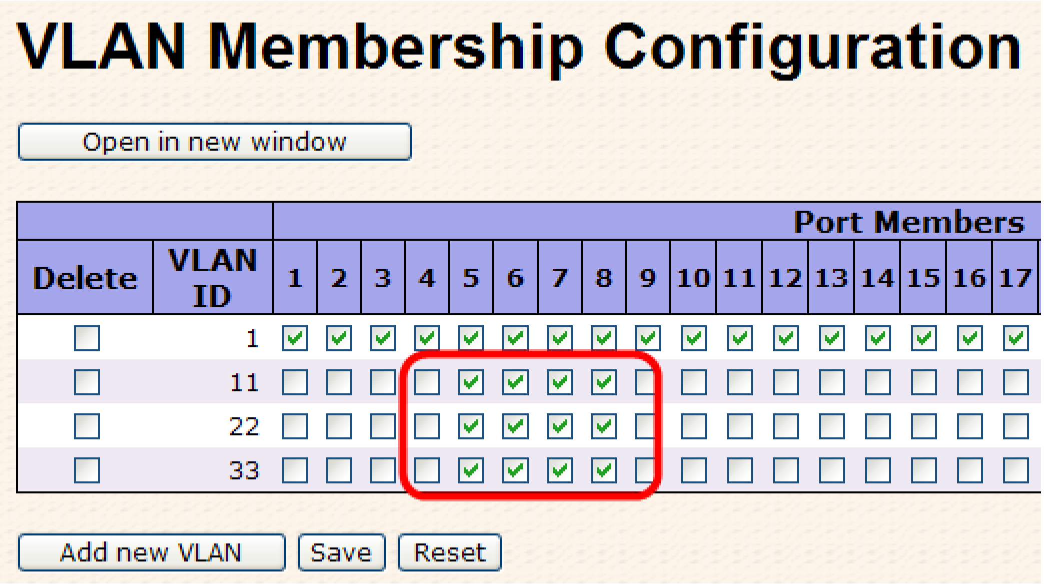


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	☑	All	Specific	11
2	☑	All	Specific	1
3	☑	All	Specific	1
4	☑	All	Specific	1
5	□	All	Specific	1

(For egress port)

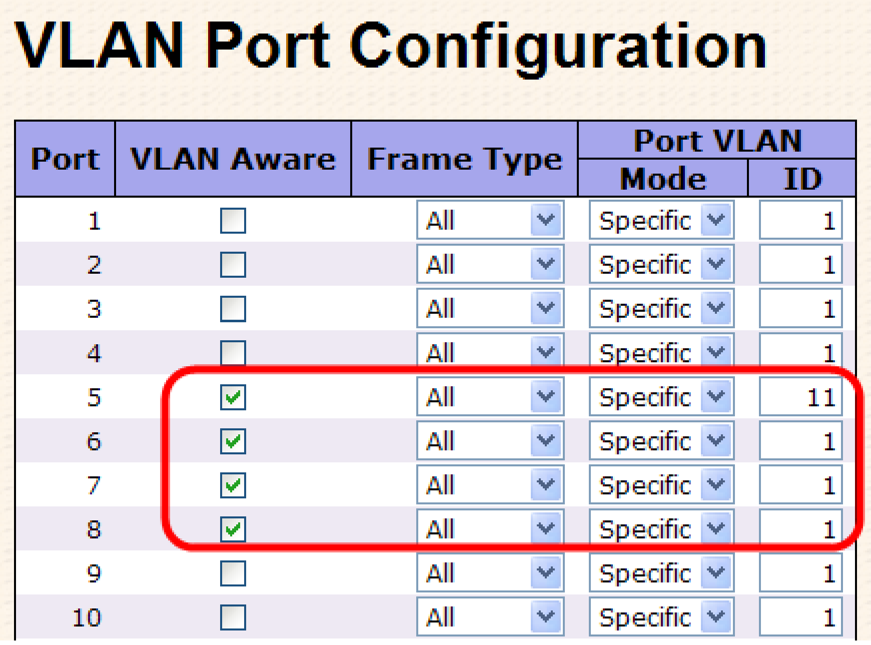
1. VLAN Membership Configuration setting port, VID=11,22,33



VLAN Membership Configuration

		Port Members																
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	11	□	□	□	□	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□
□	22	□	□	□	□	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□
□	33	□	□	□	□	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□

2. VLAN Port Configuration-->Enable VLAN Aware



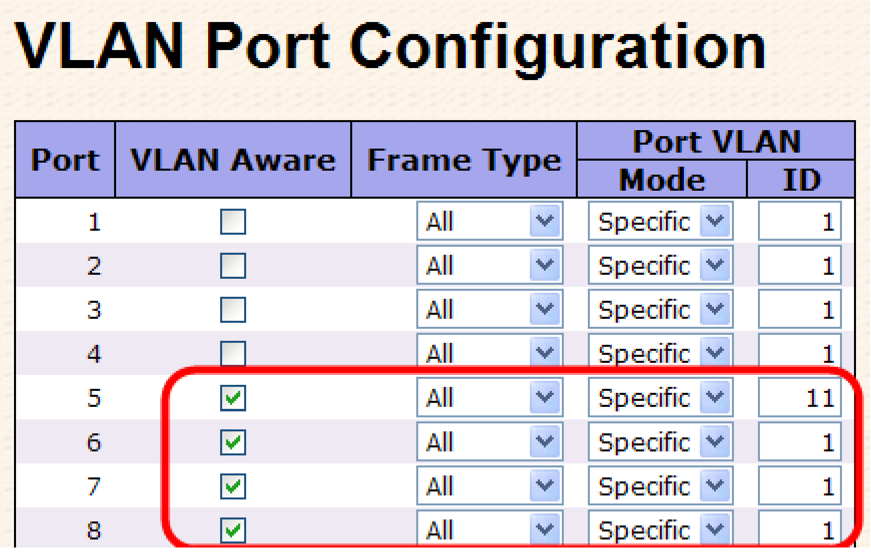
VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	1
2	□	All	Specific	1
3	□	All	Specific	1
4	□	All	Specific	1
5	☑	All	Specific	11
6	☑	All	Specific	1
7	☑	All	Specific	1
8	☑	All	Specific	1
9	□	All	Specific	1
10	□	All	Specific	1

3. VLAN Port Configuration-->Mode=none

(egress port can receive tag=11,22,33 packet

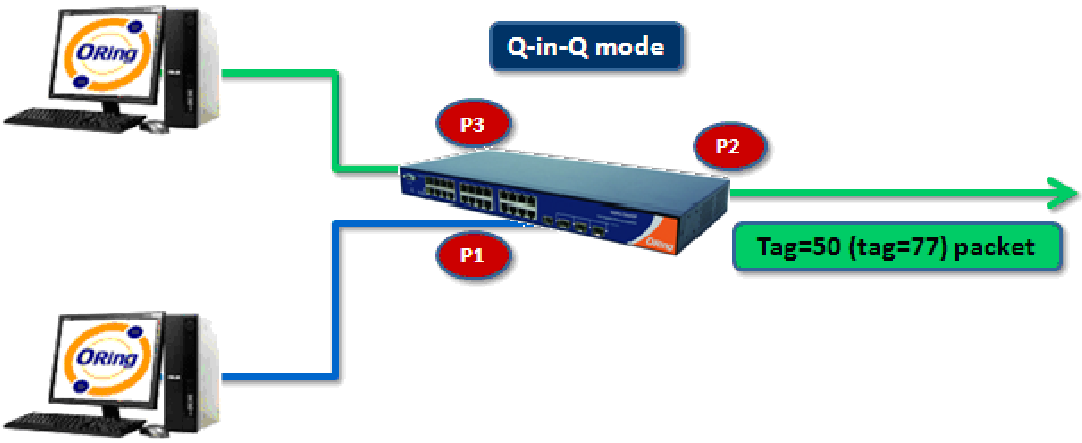
In addition ,ony tag=11packet can enter egress port)



VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	1
2	□	All	Specific	1
3	□	All	Specific	1
4	□	All	Specific	1
5	☑	All	Specific	11
6	☑	All	Specific	1
7	☑	All	Specific	1
8	☑	All	Specific	1

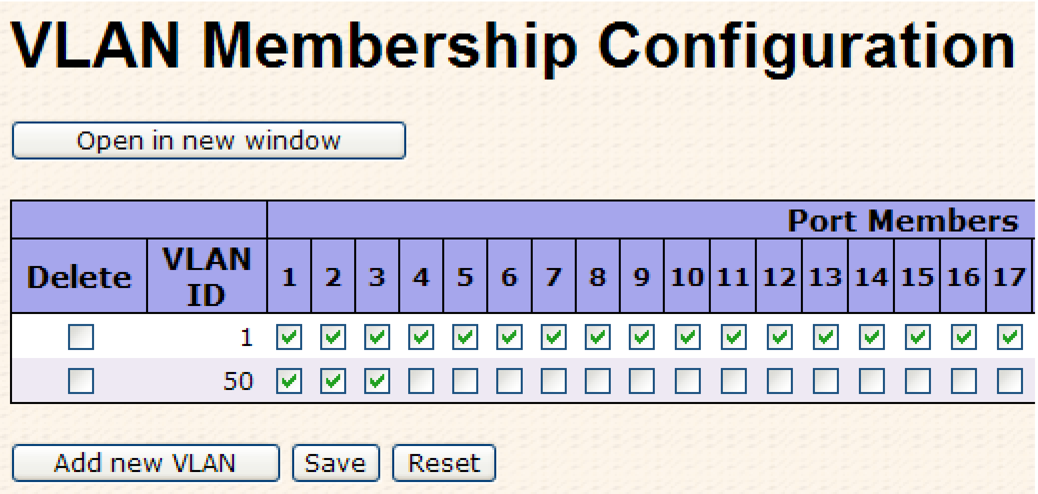
QinQ VLAN Setting



ingress Port 1------------------->egress Port 2

(For ingress port-----Port 1)

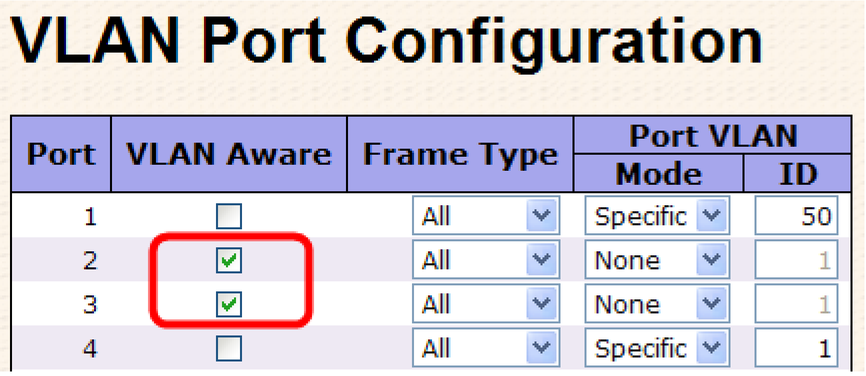
1. VLAN Membership Configuration setting port 1、2、3 & VID=50



VLAN Membership Configuration

		Port Members																
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	50	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□

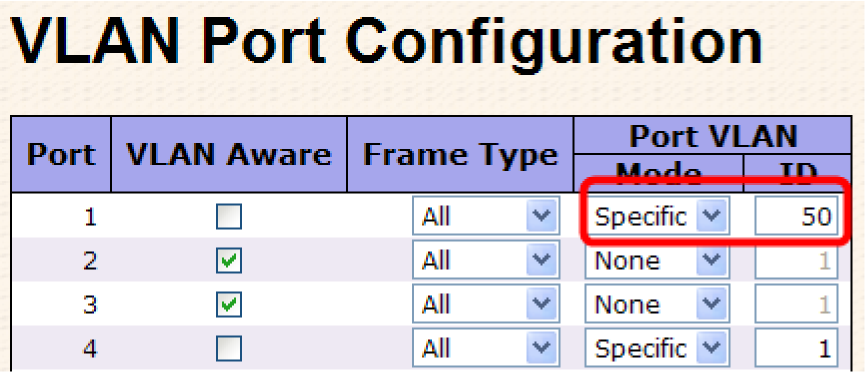
2. VLAN Port Configuration-->Disable Port 1 VLAN Aware



VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	□	All	Specific	50
2	☑	All	None	1
3	☑	All	None	1
4	□	All	Specific	1

3. VLAN Port Configuration-->Port 1 Mode=specific,ID=50

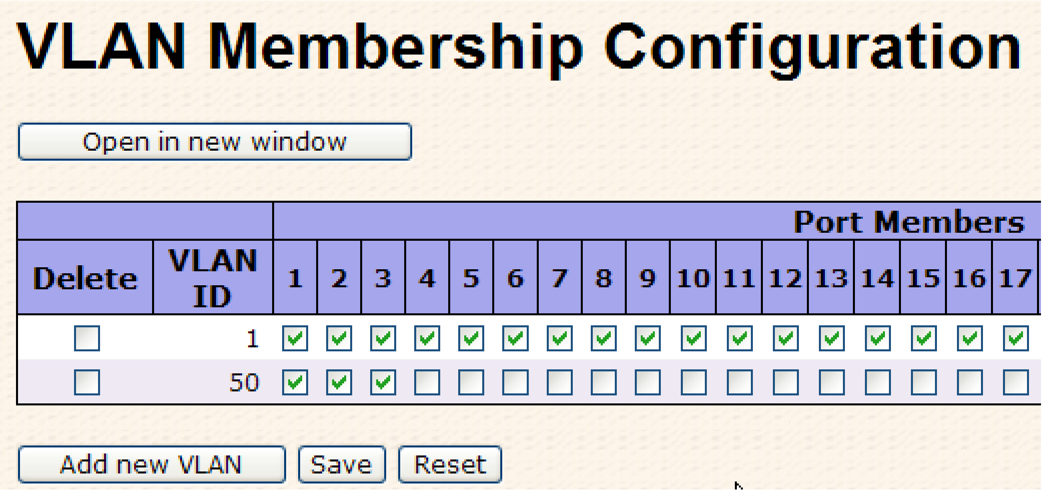


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	Port VLAN ID
1	□	All	Specific	50
2	☑	All	None	1
3	☑	All	None	1
4	□	All	Specific	1

(For egress port ----Port 2)

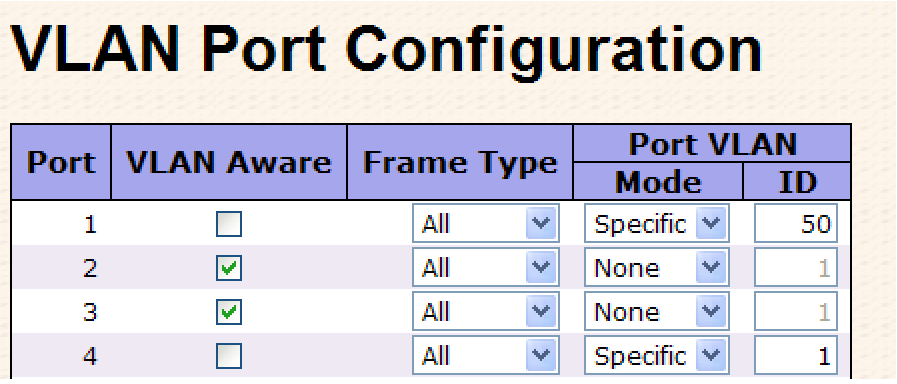
1. VLAN Membership Configuration setting port & VID=50



VLAN Membership Configuration

Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	50	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□

2. VLAN Port Configuration-->Enable Port 2、3 VLAN Aware.

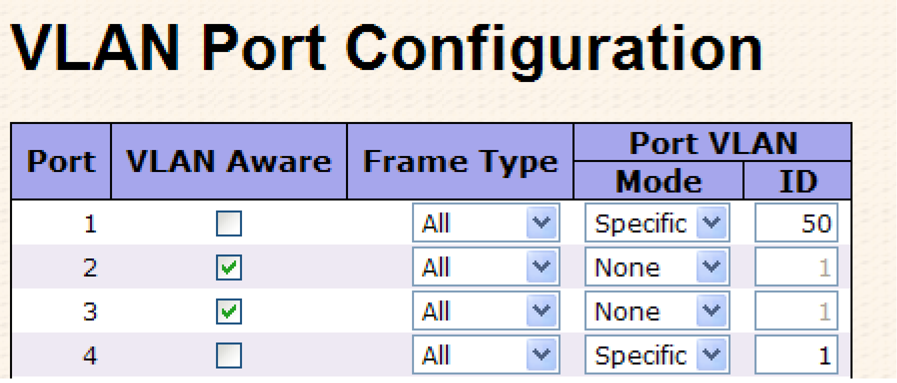


VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	Port VLAN ID
1	□	All	Specific	50
2	☑	All	None	1
3	☑	All	None	1
4	□	All	Specific	1

3. VLAN Port Configuration-->Mode=none

(only tag=50 packet can enter egress port)



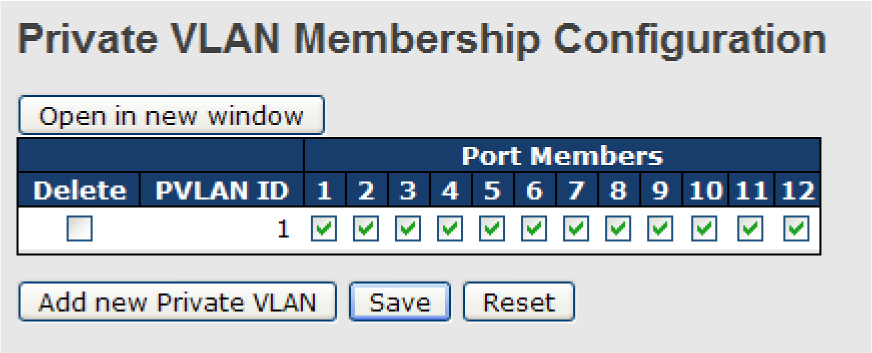
VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	Port VLAN ID
1	□	All	Specific	50
2	☑	All	None	1
3	☑	All	None	1
4	□	All	Specific	1

5.1.6.2 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

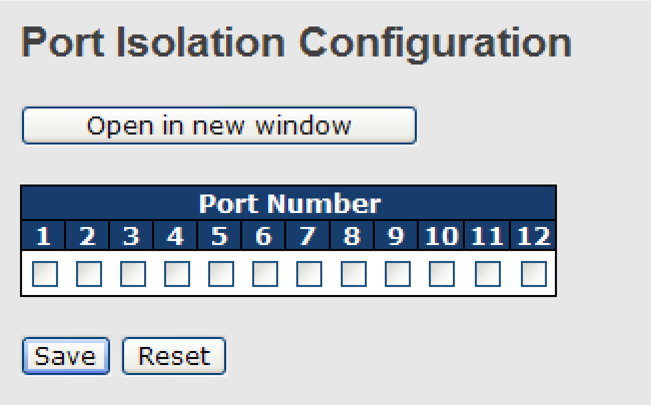


Private VLAN Membership Configuration

		Port Members											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all

	boxes are unchecked.
Adding a New Static Entry	Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The Delete button can be used to undo the addition of new Private VLANs.

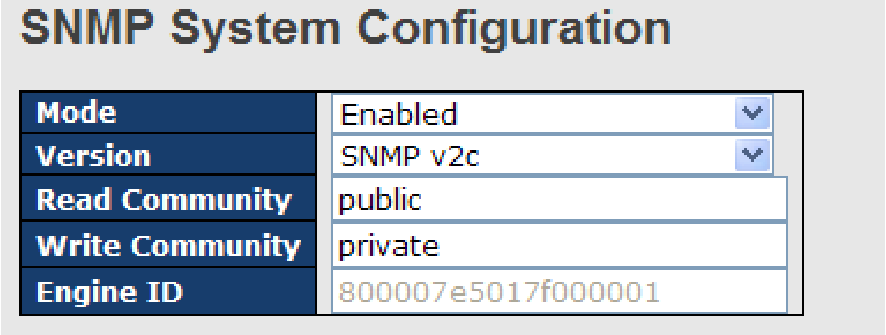

Port Isolation Configuration

Port Number											
1	2	3	4	5	6	7	8	9	10	11	12
□	□	□	□	□	□	□	□	□	□	□	□

Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

5.1.7 SNMP

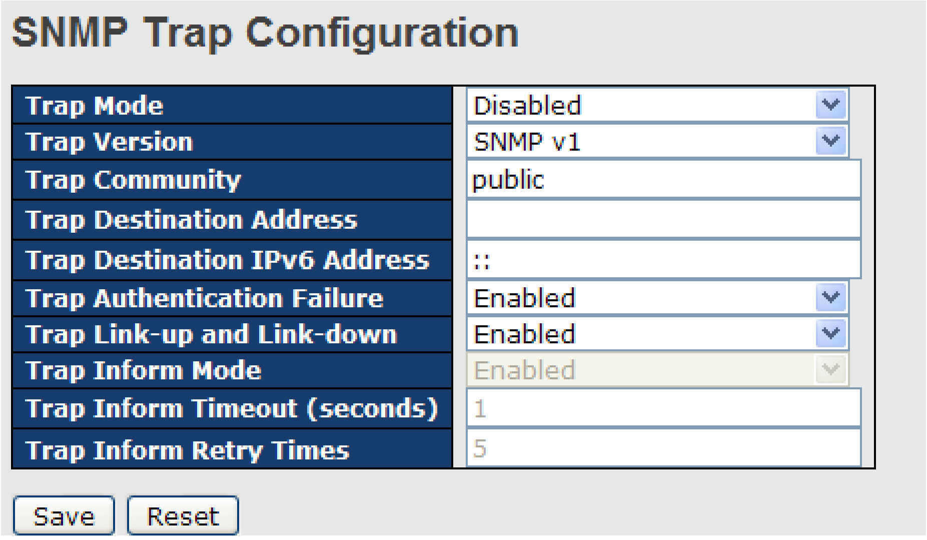
5.1.7.1 SNMP-System



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table
Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.



SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Destination IPv6 Address	::
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

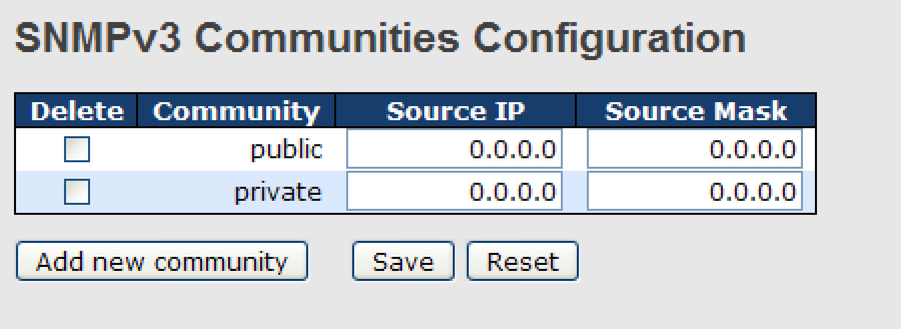
Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. Trap Destination IPv6 Address
Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and	Indicates the SNMP trap link-up and link-down mode operation.

Link-down	Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

5.1.7.2 SNMP-Communities

Configure SNMPv3 communities table on this page. The entry index key is Community.



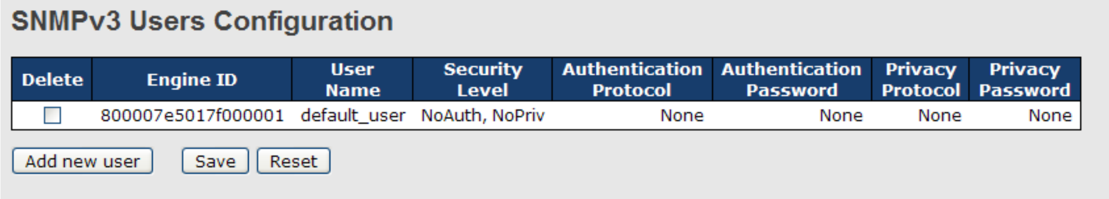
SNMPv3 Communities Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

5.1.7.3 SNMP-Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.



SNMPv3 Users Configuration

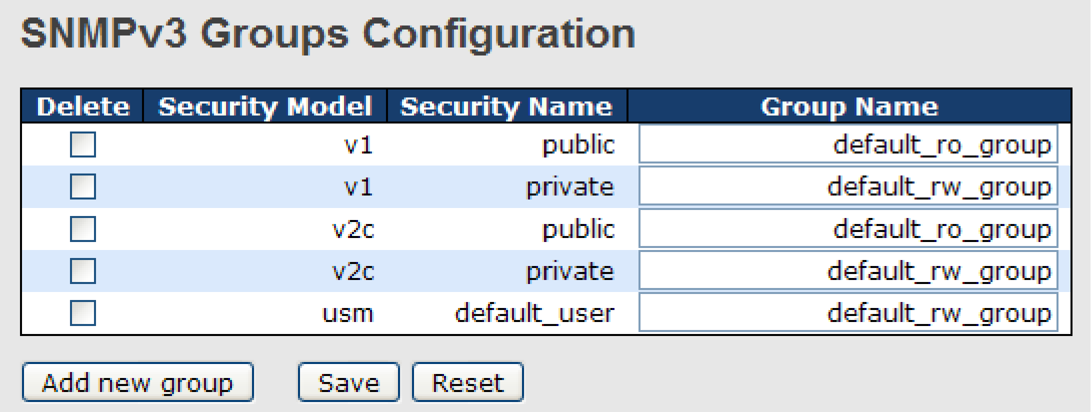
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value.

	The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In othe words, if user engine ID equal system engine ID then it is local user; otherwize it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

5.1.7.4 SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.



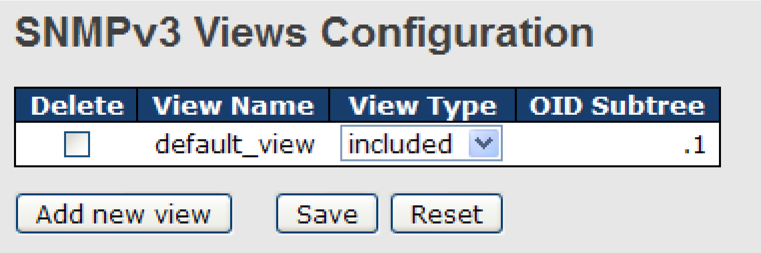
SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

5.1.7.5 SNMP-Views

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.



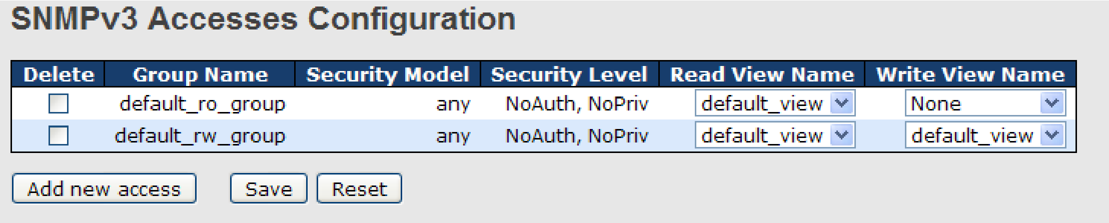
SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

5.1.7.6 SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.



SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.

Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Accepted any security model (v1|v2c|usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

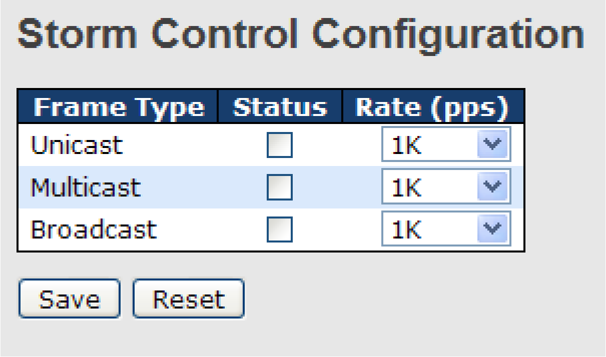
5.1.8 Traffic Prioritization

5.1.8.1 Stom Control

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: Frames, which are sent to the CPU of the switch are always limited to aproximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.



Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	□	1K
Multicast	□	1K
Broadcast	□	1K

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

5.1.8.2 Port QoS

This page allows you to configure QoS settings for each port.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QCL that is assigned to each port.

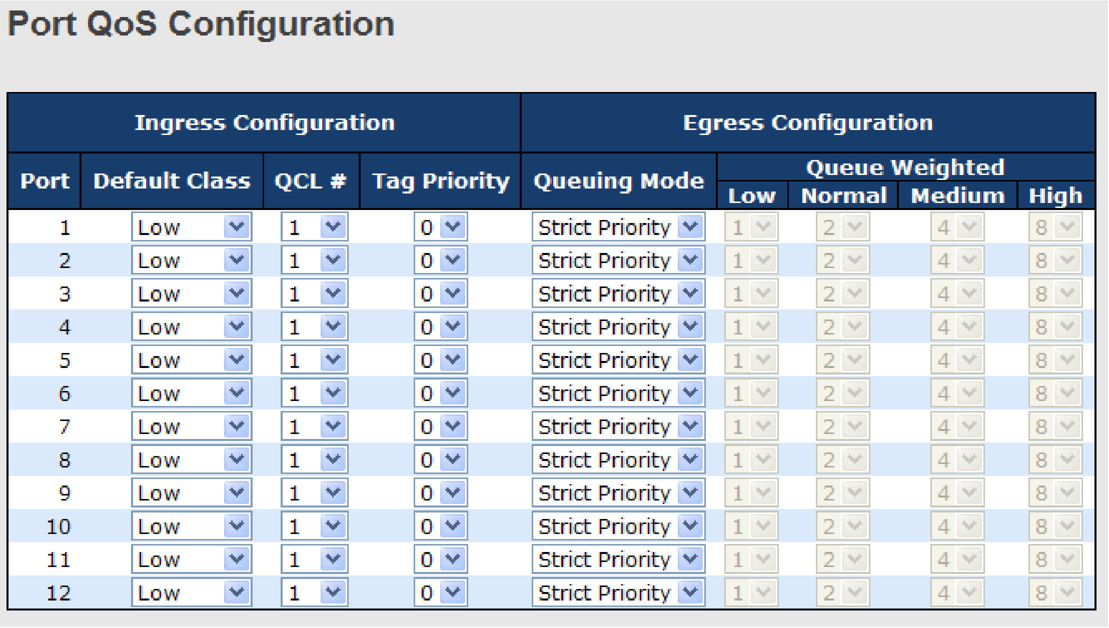
A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

Frames not matching any of the QCEs are classified to the default QoS class for the port.

Port QoS Configuration



Port QoS Configuration

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8

Label	Description
Port	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL#	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Queuing Mode	Select which Queuing mode for this port.
Queue Weighted	Setting Queue weighted (Low=Normal, Medium=High) if the "Queuing Mode" is "Weighted".

5.1.8.3 QoS Control List

This page lists the QCEs for a given QCL.

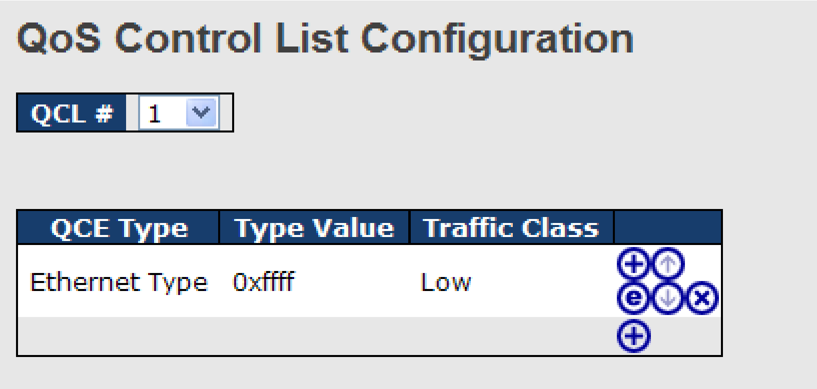
Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QoS assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.



QoS Control List Configuration

QCL # 1

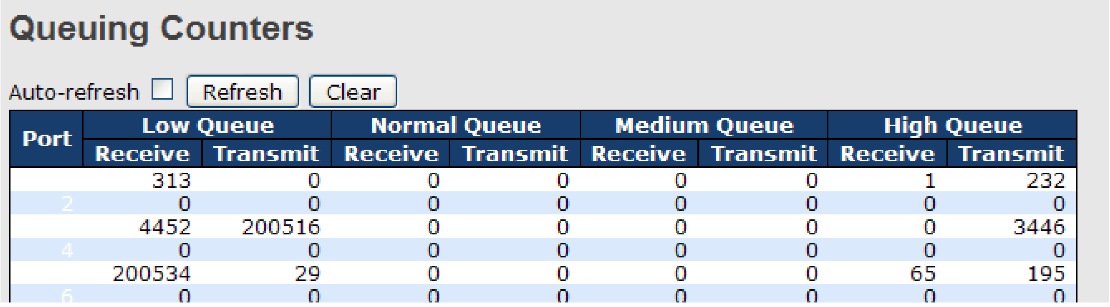
QCE Type	Type Value	Traffic Class	
Ethernet Type	0xffff	Low	⊕ ⊕ ⓔ ⊗
			⊕

Label	Description
QCL#	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Tyep	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header. VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged. TCP/UDP Port: IPv4 TCP/UDP source/destination port. DSCP: IPv4 and IPv6 DSCP. ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field). Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.
Type Value	Indicates the value according to its QCE type. Ethernet Type: The field shows the Ethernet Type value. VLAN ID: The field shows the VLAN ID. TCP/UDP Port: The field shows the TCP/UDP port range. DSCP: The field shows the IPv4/IPv6 DSCP value.
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	You can modify each QCE in the table using the following buttons: ⊕ : Inserts a new QCE before the current row.

	ⓔ : Edits the QCE. ↑ : Moves the QCE up the list. ↓ : Moves the QCE down the list. ⊗ : Deletes the QCE. ⊕ : The lowest plus sign adds a new entry at the bottom of the list of QCL.

5.1.8.4 Queuing Counters

This page provides statistics for the different queues for all switch ports.



Queuing Counters

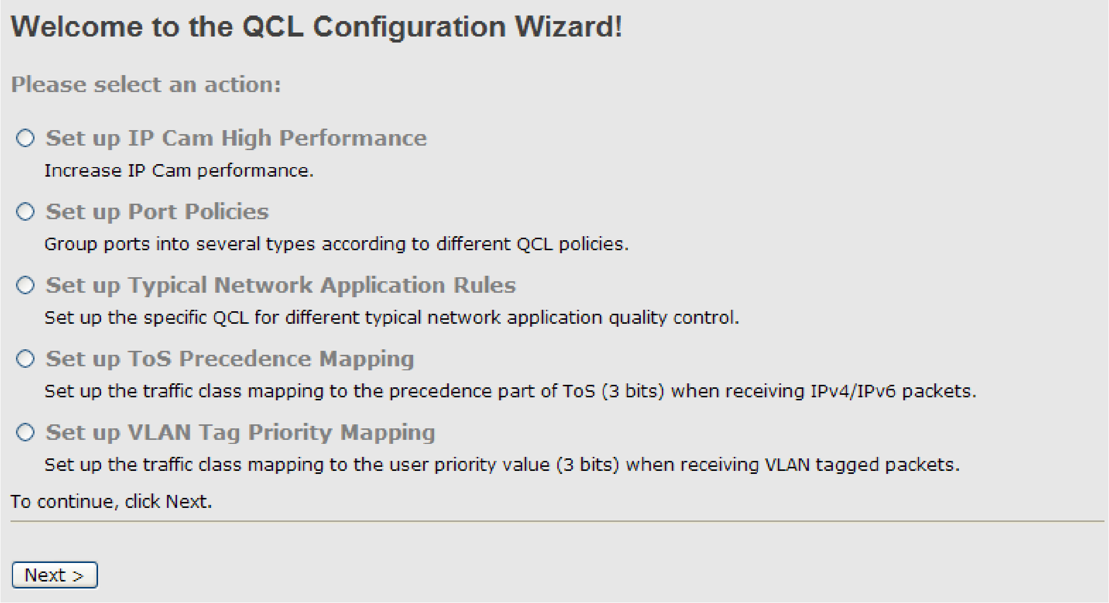
Auto-refresh □

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
	313	0	0	0	0	0	1	232
2	0	0	0	0	0	0	0	0
	4452	200516	0	0	0	0	0	3446
4	0	0	0	0	0	0	0	0
	200534	29	0	0	0	0	65	195
6	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive / Transmit	The number of received and transmitted packets per port.

5.1.8.5 Wizard

This handy wizard helps you set up a QCL quickly.



Welcome to the QCL Configuration Wizard!

Please select an action:

○ Set up IP Cam High Performance
Increase IP Cam performance.

○ Set up Port Policies
Group ports into several types according to different QCL policies.

○ Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control.

○ Set up ToS Precedence Mapping
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

○ Set up VLAN Tag Priority Mapping
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

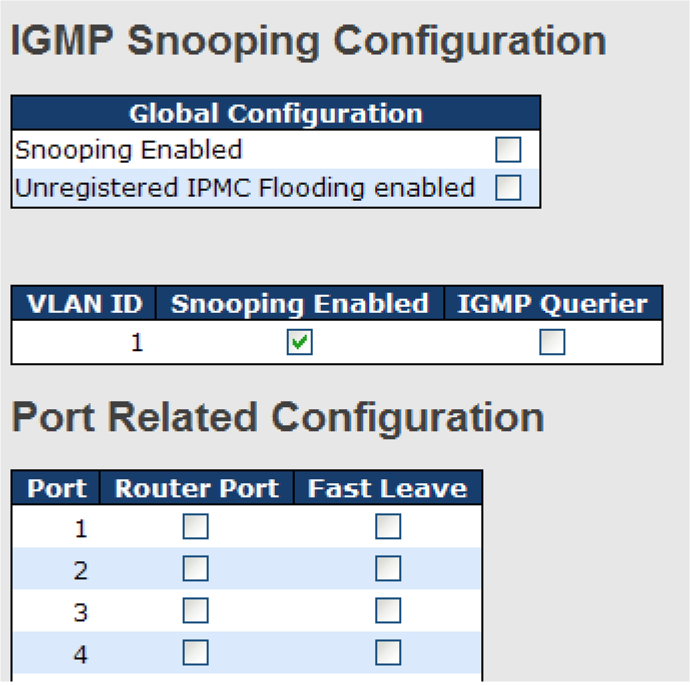
To continue, click Next.

Label	Description
Set up Port Policies	Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules	Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

5.1.9 Multicast

5.1.9.1 IGMP Snooping

This page provides IGMP Snooping related configuration.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMC Flooding enabled	□

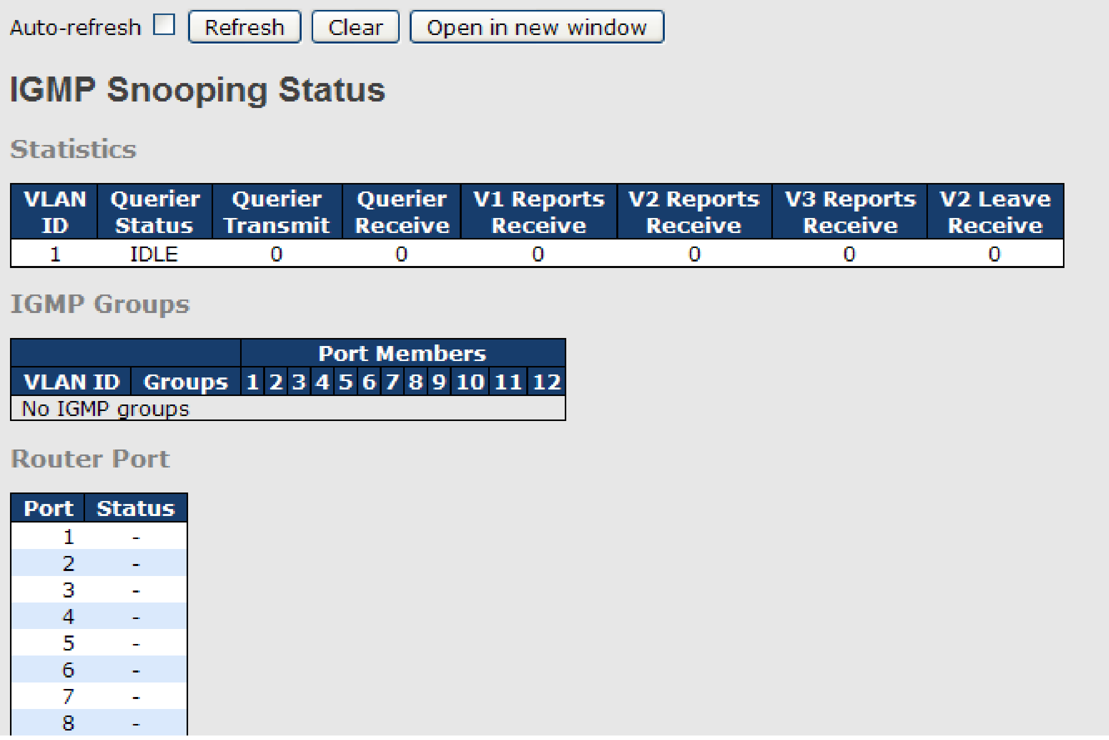
VLAN ID	Snooping Enabled	IGMP Querier
1	☑	□

Port Related Configuration

Port	Router Port	Fast Leave
1	□	□
2	□	□
3	□	□
4	□	□

Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

5.1.9.2 IGMP Snooping Status



Auto-refresh □ Refresh Clear Open in new window

IGMP Snooping Status

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
1	IDLE	0	0	0	0	0	0

IGMP Groups

		Port Members											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12
No IGMP groups													

Router Port

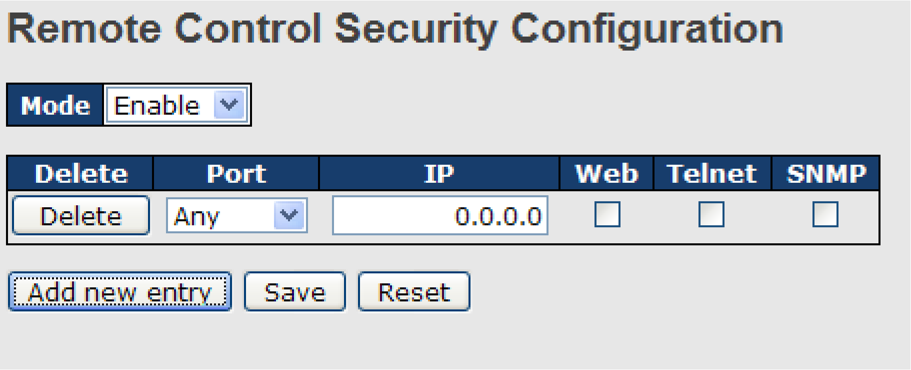
Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Groups	The present IGMP groups. Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.10 Security

5.1.10.1 Remote Control Security Configuration

Remote Control Security allows you limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.



Remote Control Security Configuration

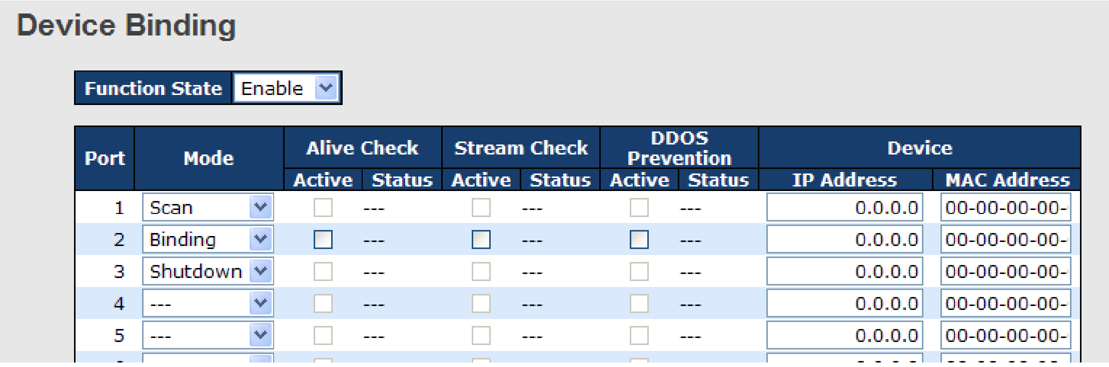
Mode: Enable

Delete	Port	IP	Web	Telnet	SNMP
Delete	Any	0.0.0.0	□	□	□

Label	Description
Port	Port number of remote client.
IP Address	IP address of remote client. Keeps this field "0.0.0.0" means "Any IP".
Web	Check this item to enable Web management interface.
Telnet	Check this item to enable Telnet management interface.
SNMP	Check this item to enable SNMP management interface
Delete	Check this item to delete.

5.1.10.2 Device Binding

This page provides Device Binding related configuration. Device Binding is an powerful monitor for devices and network security.



Device Binding

Function State: Enable

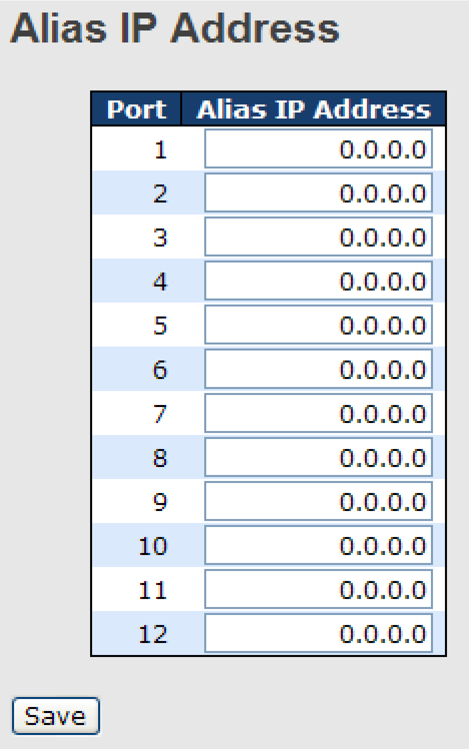
Port	Mode	Alive Check		Stream Check		DDOS Prevention		Device	
		Active	Status	Active	Status	Active	Status	IP Address	MAC Address
1	Scan	□	---	□	---	□	---	0.0.0.0	00-00-00-00-
2	Binding	□	---	□	---	□	---	0.0.0.0	00-00-00-00-
3	Shutdown	□	---	□	---	□	---	0.0.0.0	00-00-00-00-
4	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-
5	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-

Label	Description
Mode	Indicates the per-port Device Binding operation. Possible modes are: ---: Disable. Scan: Scan IP/MAC automatically, but no binding function. Binding: Enable binding function. Under this mode, any IP/MAC doesn't match the entry will not be allowed to access the network. Shutdown: Shutdown the port (No Link).
Alive Check Active	Enable/Disable Alive Check. When enabled, switch will ping the device continually.
Alive Check Satus	Indicates the Alive Check status. Possible statuses are: ---: Disable. Got Reply: Got ping reply from device, that means the device is still alive. Lost Reply: Lost ping reply from device, that means the device might have been hanged.
Stream Check Active	Enable/Disable Stream Check. When enabled, switch will detect the stream change(getting low) from device.
Stream Check Status	Indicates the Stream Check status. Possible statuses are: ---: Disable. Normal: The stream is normal. Low: The stream is getting low.
DDoS Prevention Acton	Enable/Disable DDOS Prevention. When enabled, switch will monitor the device to against DDOS attack (from device).
DDoS Prevention Status	Indicates the DDOS Prevention status. Possible statuses are: ---: Disable. Analysing: Analyse the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.
Device IP Address	Specify the IP Address of device.
Device MAC Address	Specify the MAC Address of device.

4.1.10.2.1 Advanced Configuration

Alias IP Address

This page provides Alias IP Address related configuration. Some device might have more IP addresses than one, you could specify the other IP address here.



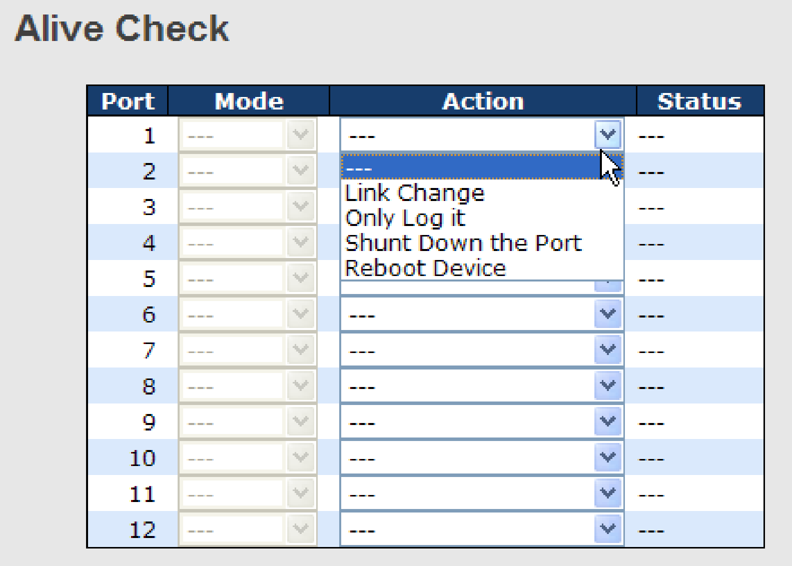
Alias IP Address

Port	Alias IP Address
1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0
5	0.0.0.0
6	0.0.0.0
7	0.0.0.0
8	0.0.0.0
9	0.0.0.0
10	0.0.0.0
11	0.0.0.0
12	0.0.0.0

Label	Description
Alias IP Address	Specify Alias IP address. Keeps "0.0.0.0", if the device doesn't have alias IP address.

Alive Check

using the ping command ,check port link status, if port link fail .user can setting action field , select the switch action.



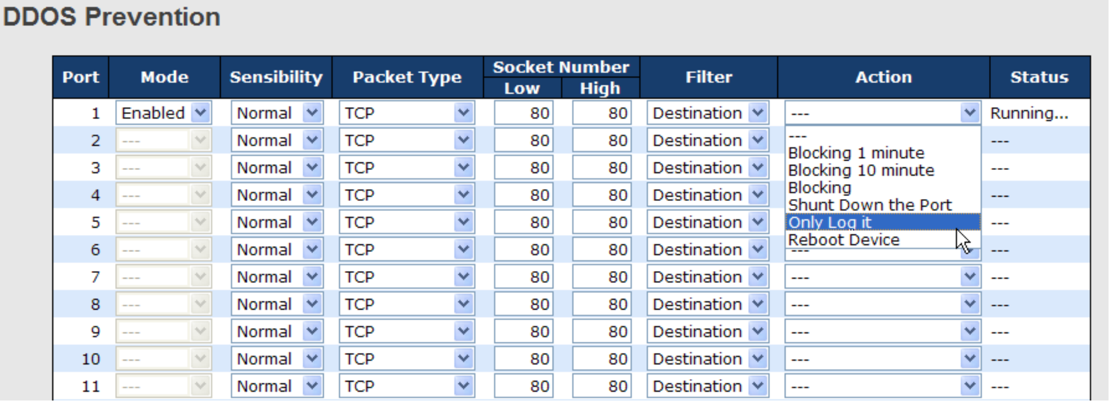
Alive Check

Port	Mode	Action	Status
1	---	---	---
2	---		---
3	---		---
4	---		---
5	---		---
6	---	---	---
7	---	---	---
8	---	---	---
9	---	---	---
10	---	---	---
11	---	---	---
12	---	---	---

Label	Description
Link Change	Disable and enable port .
Only log it	Only sent log to log server .
Shunt Down the Port	Disable this port .
Reboot Device	Disable and Enable P.O.E Power ,

DDoS Prevention

This page provides DDOS Prevention related configuration. Switch could monitor the ingress packets, and do some actions when DDOS attack happened on this port. Configure these setting helps the prevention become more suitable.



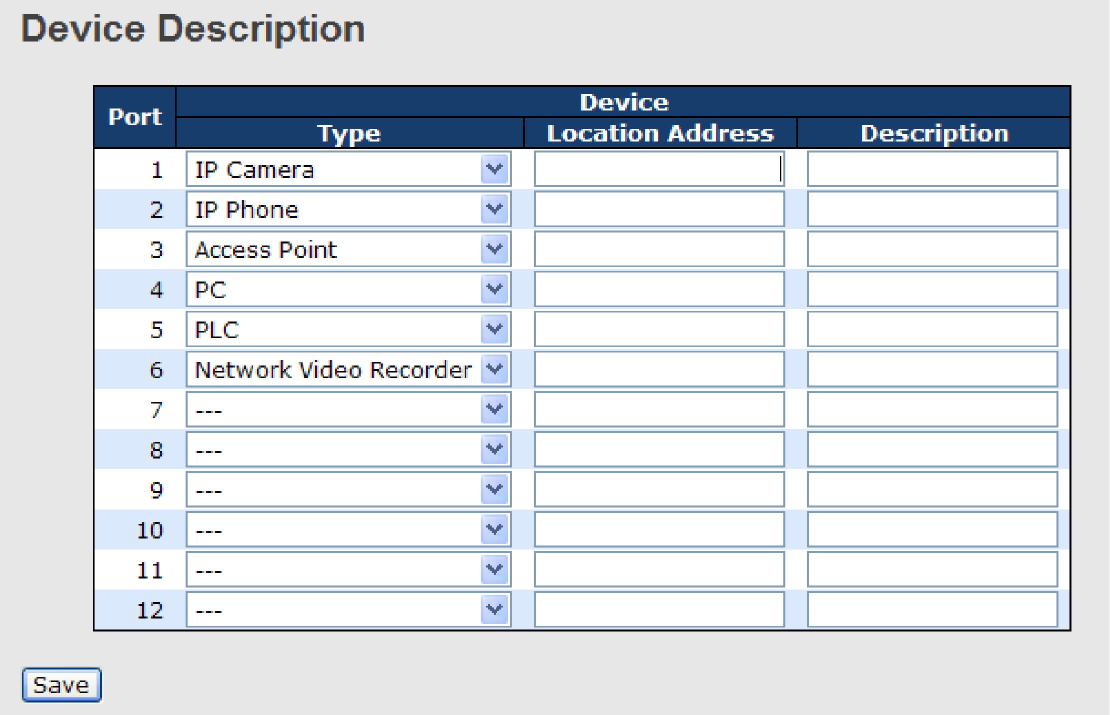
DDOS Prevention

Port	Mode	Sensibility	Packet Type	Socket Number		Filter	Action	Status
				Low	High			
1	Enabled	Normal	TCP	80	80	Destination	---	Running...
2	---	Normal	TCP	80	80	Destination		---
3	---	Normal	TCP	80	80	Destination		---
4	---	Normal	TCP	80	80	Destination		---
5	---	Normal	TCP	80	80	Destination		---
6	---	Normal	TCP	80	80	Destination		---
7	---	Normal	TCP	80	80	Destination	---	---
8	---	Normal	TCP	80	80	Destination	---	---
9	---	Normal	TCP	80	80	Destination	---	---
10	---	Normal	TCP	80	80	Destination	---	---
11	---	Normal	TCP	80	80	Destination	---	---

Label	Description
Mode	Enable/Disable DDOS Prevention of the port.
Sensibility	Indicates the level of DDOS detection. Possible levels are: Low: Low sensibility. Normal: Normal sensibility. Medium: Medium sensibility. High: High sensibility.
Packet Type	Indicates the packet type of DDOS monitor. Possible types are: RX Total: Total ingress packets. RX Unicast: Unicast ingress packets. RX Multicast: Multicast ingress packets. RX Broadcast: Broadcast ingress packets. TCP: TCP ingress packets. UDP: UDP ingress packets.
Socket Number	If packet type is UDP(or TCP), please specify the socket number here. The socket number could be a range, from low to high. If the socket number is only one, please fill the same number in low field and high field.
Filiter	If packet type is UDP(or TCP), please choose the socket direction (Destination/Source).
Action	Indicates the action when DDOS attack happened. Possible actions are: ---: Do nothing. Blocking 1 minute: To block the forwarding for 1 mintue, and log the event. Blocking 10 minute: To block the forwarding for 10 mintues, and log the event. Blocking: Just blocking, and log the event. Shunt Down the Port: Shut down the port(No Link), and log the event. Only Log it: Just log the event. Reboot Device: If POE supported, the device could be rebooted. And log the event.
Status	Indicates the DDOS Prevention status. Possible statuses are: ---: Disable. Analysing: Analyse the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.

Device Description

This page provides Device Description related configuration



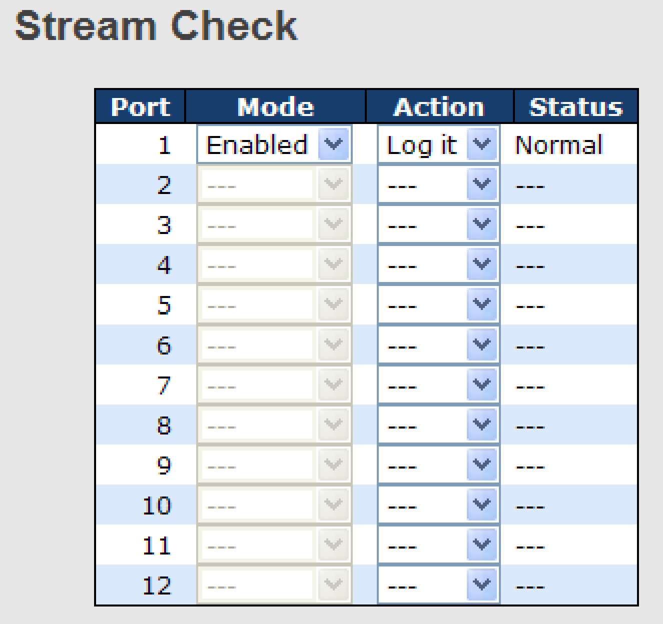
Device Description

Port	Device Type	Device Location Address	Device Description
1	IP Camera		
2	IP Phone		
3	Access Point		
4	PC		
5	PLC		
6	Network Video Recorder		
7	---		
8	---		
9	---		
10	---		
11	---		
12	---		

Label	Description
Device Type	Indicates the type of device. Possible types are: ---: No specification. IP Camera: IP Camera. IP Phone: IP Phone. Access Point: Access Point. PC: PC. PLC: PLC. Network Video Recorder: Network Video Recorder.
Location Address	Location information of device, this information could be used for Google Mapping.
Description	Device description.

Stream Check

This page provides Stream Check related configuration.



Stream Check

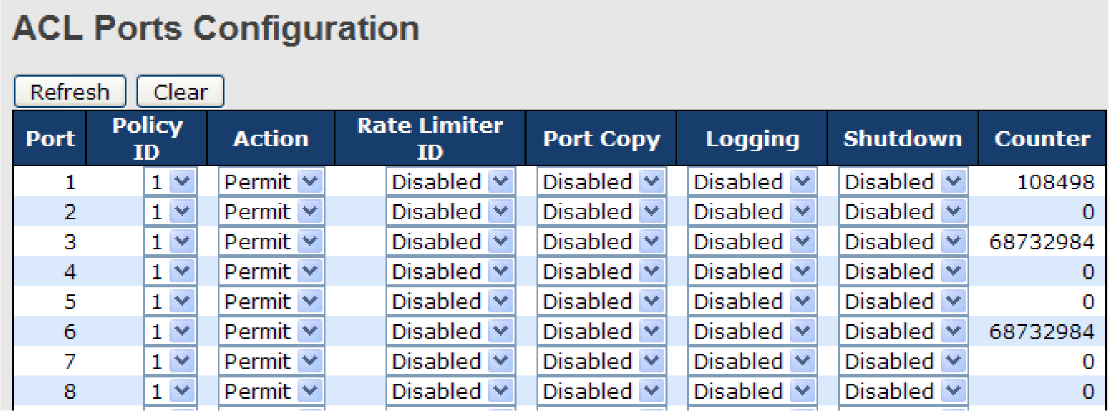
Port	Mode	Action	Status
1	Enabled	Log it	Normal
2	---	---	---
3	---	---	---
4	---	---	---
5	---	---	---
6	---	---	---
7	---	---	---
8	---	---	---
9	---	---	---
10	---	---	---
11	---	---	---
12	---	---	---

Label	Description
Mode	Enable/Disable stream monitor of the port.
Action	Indicates the action when stream getting low. Possible actions are: ---: Do nothing. Log it: Just log the event

5.1.10.3 ACL

5.1.10.3.1 Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



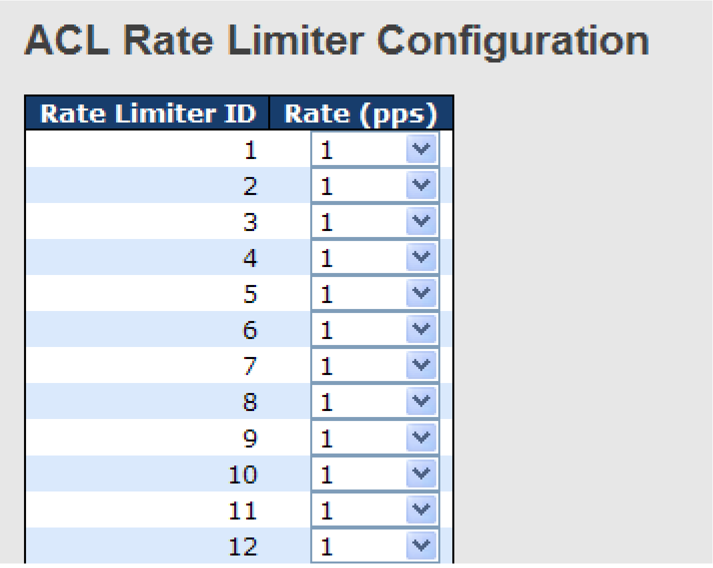
ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	108498
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	68732984
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	68732984
7	1	Permit	Disabled	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

5.1.10.3.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1

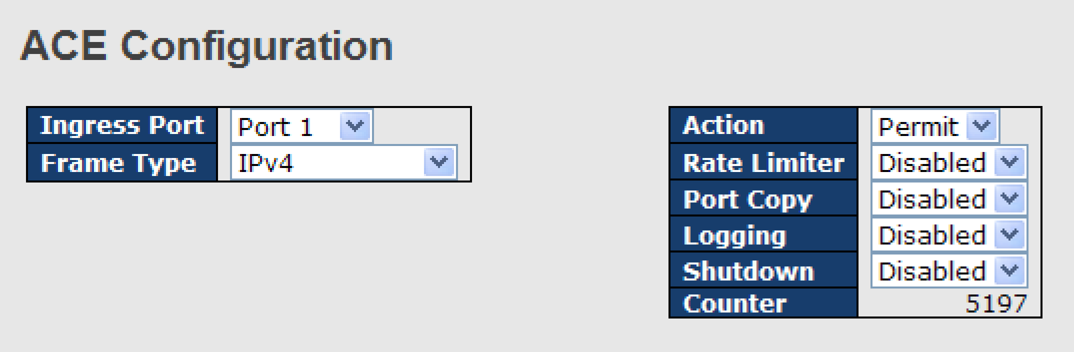
Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

5.1.10.3.3 ACL Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

A frame that hits this ACE matches the configuration that is defined here.

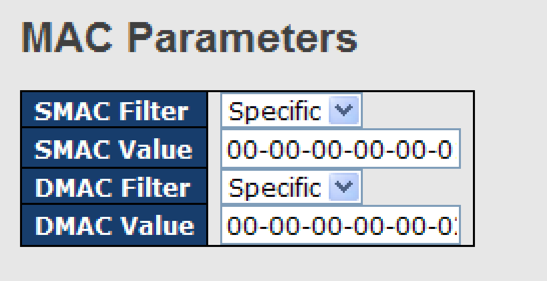

ACE Configuration

Ingress Port	Port 1
Frame Type	IPv4

Action	Permit
Rate Limiter	Disabled
Port Copy	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	5197

Label	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port. Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 descripts the value of Length/Type Field specifications

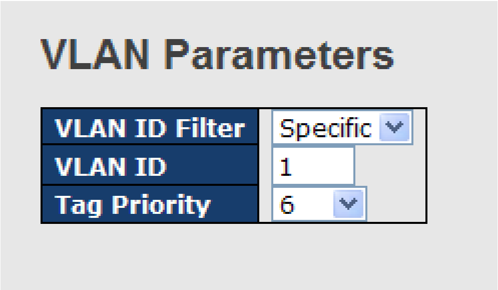
	should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with etnernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with etnernet type.
Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.



MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-0
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-0:

Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

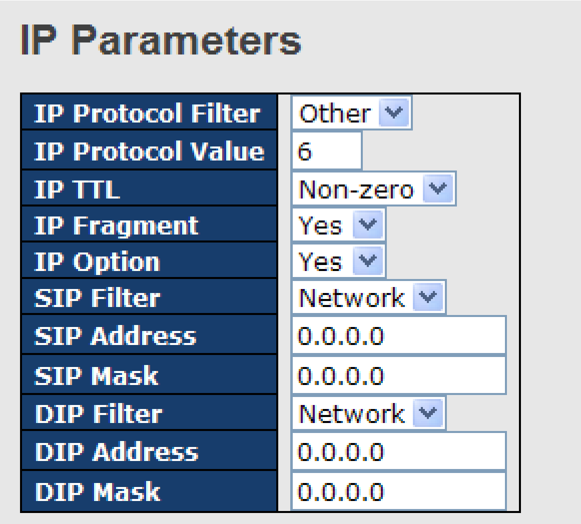


VLAN Parameters

VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	6

Label	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)



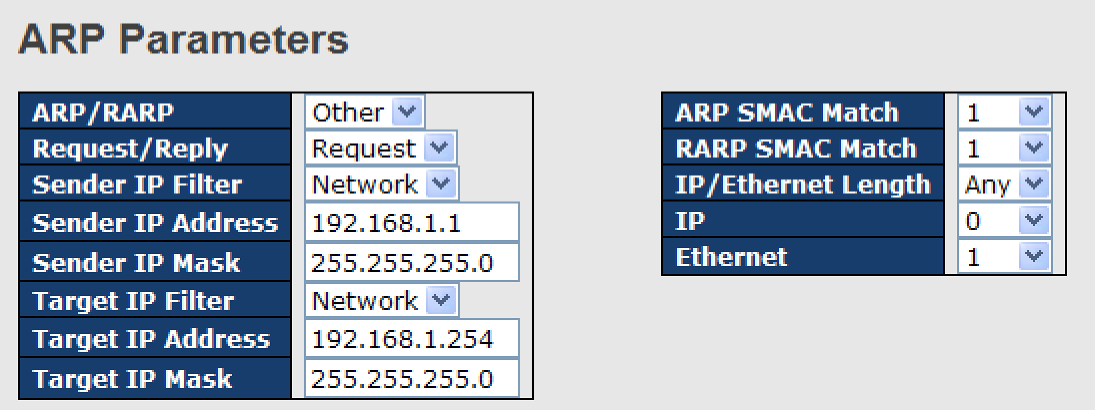
IP Parameters

IP Protocol Filter	Other
IP Protocol Value	6
IP TTL	Non-zero
IP Fragment	Yes
IP Option	Yes
SIP Filter	Network
SIP Address	0.0.0.0
SIP Mask	0.0.0.0
DIP Filter	Network
DIP Address	0.0.0.0
DIP Mask	0.0.0.0

Label	Description
IP Protocol Filter	Specify the IP protocol filter for this ACE. Any: No IP protocol filter is specified ("don't-care"). Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value.. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL	Specify the Time-to-Live settings for this ACE. zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Fragment	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. No: IPv4 frames where the options flag is set must not be able to match this entry. Yes: IPv4 frames where the options flag is set must be able to match this entry. Any: Any value is allowed ("don't-care").
SIP Filter	Specify the source IP filter for this ACE. Any: No source IP filter is specified. (Source IP filter is "don't-care".) Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specify the destination IP filter for this ACE. Any: No destination IP filter is specified. (Destination IP filter is "don't-care".) Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network: Destination IP filter is set to Network. Specify the

	destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.



ARP Parameters

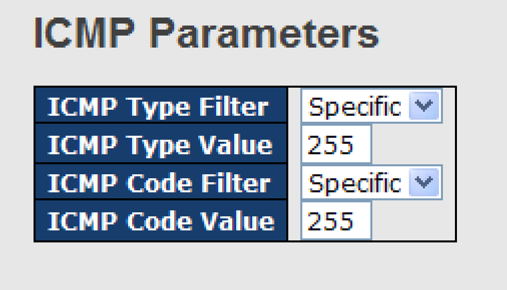
ARP/RARP	Other
Request/Reply	Request
Sender IP Filter	Network
Sender IP Address	192.168.1.1
Sender IP Mask	255.255.255.0
Target IP Filter	Network
Target IP Address	192.168.1.254
Target IP Mask	255.255.255.0

ARP SMAC Match	1
RARP SMAC Match	1
IP/Ethernet Length	Any
IP	0
Ethernet	1

Label	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can

	enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care".) Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
Target IP Adress	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
RARP SMAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the SMAC address. 1: RARP frames where THA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. 0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry. 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry. Any: Any value is allowed ("don't-care").
IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. 0: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry. 1: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry.

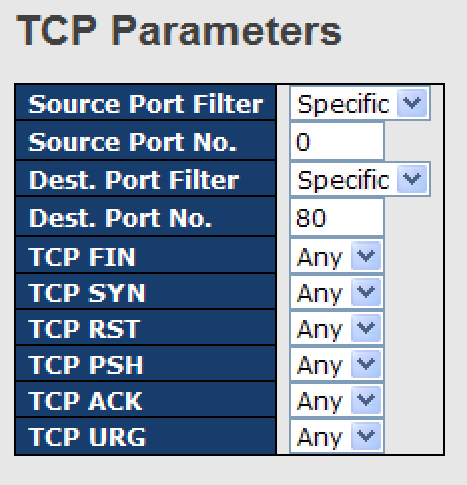
	Any: Any value is allowed ("don't-care").
Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. 0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry. 1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry. Any: Any value is allowed ("don't-care").



ICMP Parameters

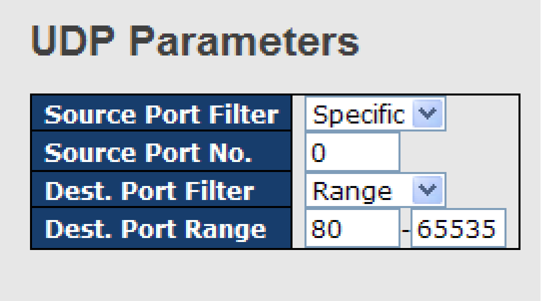
ICMP Type Filter	Specific
ICMP Type Value	255
ICMP Code Filter	Specific
ICMP Code Value	255

Label	Description
ICMP Type Filter	
ICMP Type Value	
ICMP Code Filter	
ICMP Code Value	



TCP Parameters

Source Port Filter	Specific
Source Port No.	0
Dest. Port Filter	Specific
Dest. Port No.	80
TCP FIN	Any
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any



UDP Parameters

Source Port Filter	Specific
Source Port No.	0
Dest. Port Filter	Range
Dest. Port Range	80 - 65535

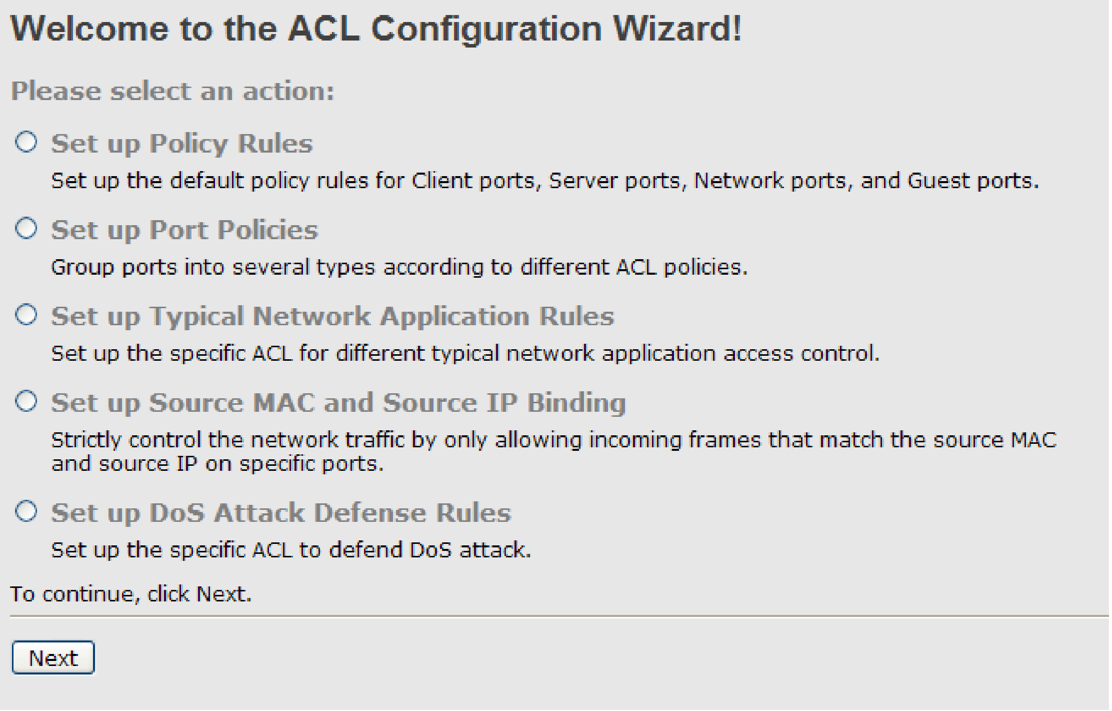
Label	Description
TCP/UDP Source	Specify the TCP/UDP source filter for this ACE.

Filter	Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
TCP/UDP Source No.	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Source Range	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
TCP/UDP Destination Number	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP/UDP Destination Range	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. 0: TCP frames where the FIN field is set must not be able to match

	this entry. 1: TCP frames where the FIN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. 0: TCP frames where the URG field is set must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry. Any: Any value is allowed ("don't-care").

5.1.10.3.4 Wizard

This handy wizard helps you set up an ACL quickly



Welcome to the ACL Configuration Wizard!

Please select an action:

○ Set up Policy Rules

Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.

○ Set up Port Policies

Group ports into several types according to different ACL policies.

○ Set up Typical Network Application Rules

Set up the specific ACL for different typical network application access control.

○ Set up Source MAC and Source IP Binding

Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.

○ Set up DoS Attack Defense Rules

Set up the specific ACL to defend DoS attack.

To continue, click Next.

Label	Description
Set up Policy Rules	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Set up Port Policies	Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules	Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
Set up Dos Attack Defense Rules	Set up the specific ACL to defend DoS attack.

5.1.10.4 802.1x

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the Authentication configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

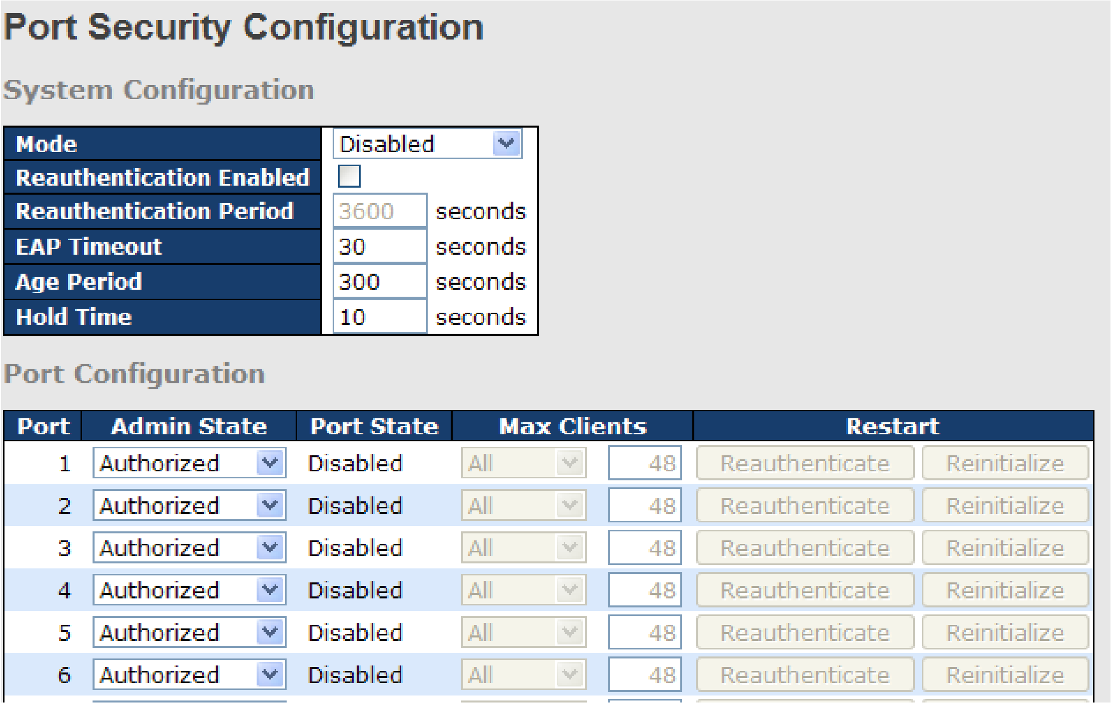
Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide



Port Security Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Port Configuration

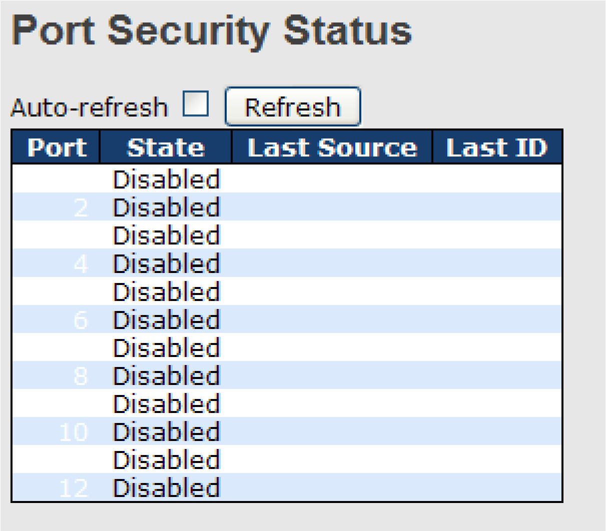
Port	Admin State	Port State	Max Clients		Restart	
1	Authorized	Disabled	All	48	Reauthenticate	Reinitialize
2	Authorized	Disabled	All	48	Reauthenticate	Reinitialize
3	Authorized	Disabled	All	48	Reauthenticate	Reinitialize
4	Authorized	Disabled	All	48	Reauthenticate	Reinitialize
5	Authorized	Disabled	All	48	Reauthenticate	Reinitialize
6	Authorized	Disabled	All	48	Reauthenticate	Reinitialize

Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAP Timeout	Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
Age Period	This setting applies to ports running MAC-based authentication,

	only. Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated.
Hold Time	This setting applies to ports running MAC-based authentication, only. If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to reauthenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access.
Port	The port number for which the configuration below applies.
Admin State	Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled): Auto: Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not

	802.1X-aware will be denied access. **Authorized:** Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up. **Unauthorized:** Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up. **MAC-Based:** Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.
Port State	The current state of the port. It can undertake one of the following values: Disabled: 802.1X and MAC-based authentication is globally disabled. Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port. Authorized: The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized". Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized". X Auth/Y Unauth: X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".
Max Clients	This setting applies to ports running MAC-based authentication, only. The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to

	consume up to 48 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 48). The switch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is "Auto" or "MAC-Based". Clicking these buttons will not cause settings changed on the page to take effect. Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized. Reinitialize: Forces a reinitialization of the port/clients and thereby a reauthentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing.



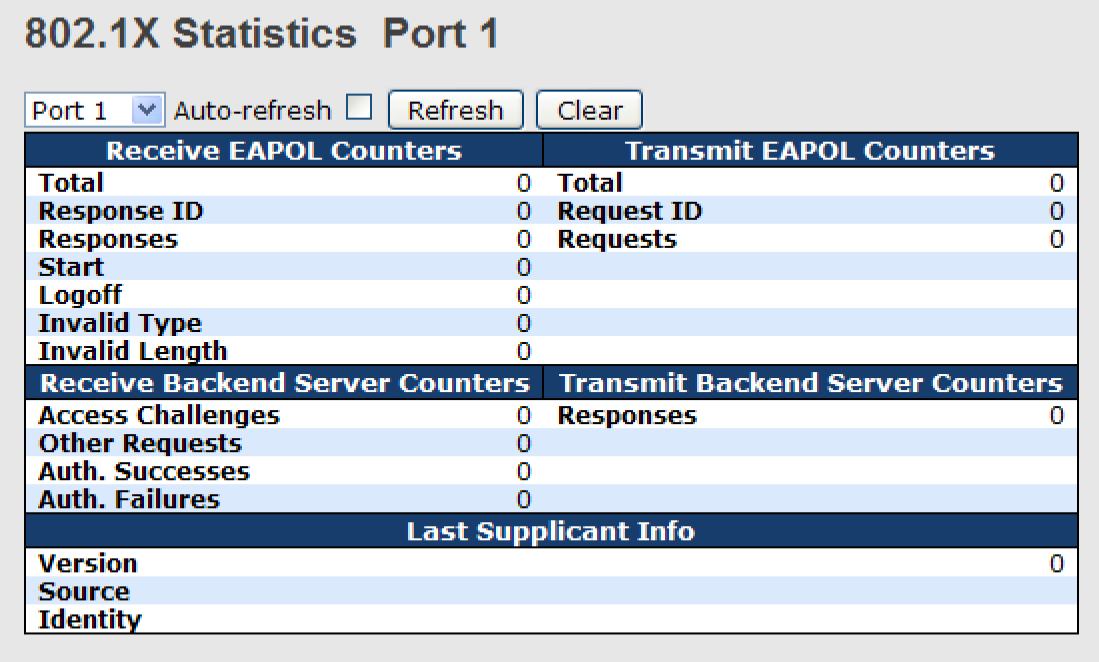
Port Security Status

Auto-refresh □ Refresh

Port	State	Last Source	Last ID
	Disabled		
2	Disabled		
	Disabled		
4	Disabled		
	Disabled		
6	Disabled		
	Disabled		
8	Disabled		
	Disabled		
10	Disabled		
	Disabled		
12	Disabled		

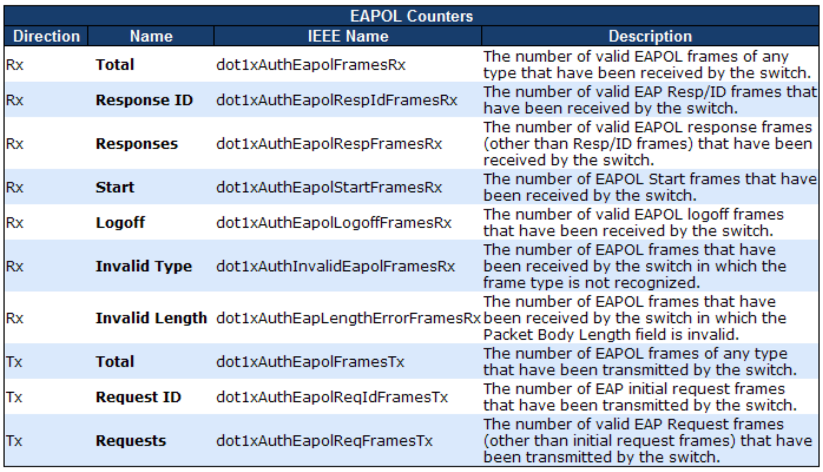
Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
State	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

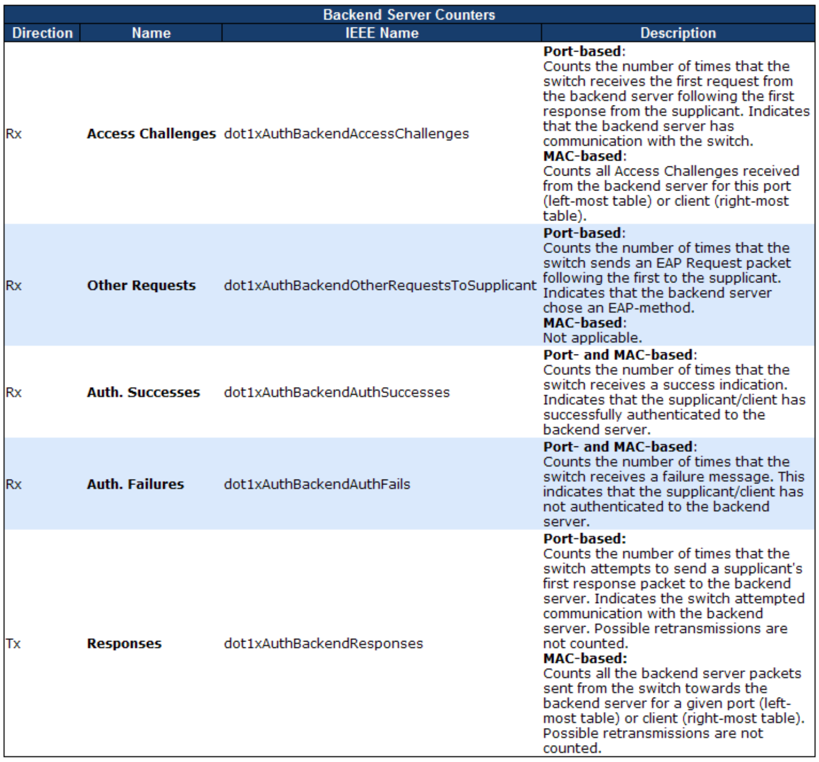
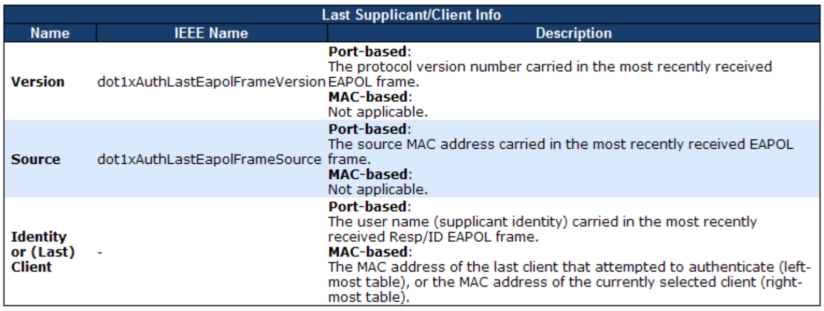
This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.



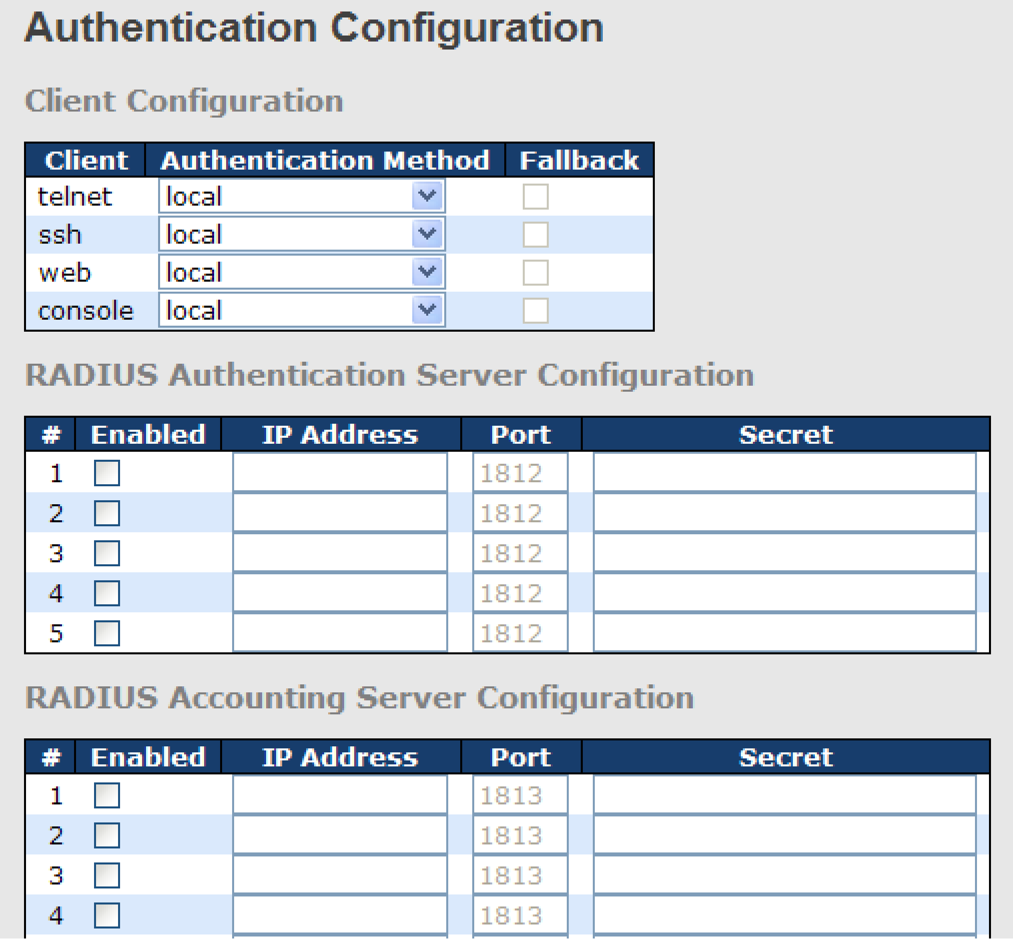
802.1X Statistics Port 1

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	0
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	0	Responses	0
Other Requests	0		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
Version			0
Source			
Identity			

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>EAPOL Counters</td><td>These counters are not available for MAC-based ports.
Supplicant frame counter statistics. There are seven receive frame counters and three transmit frame counters.

<table>
<tr><th colspan="4">EAPOL Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesRx</td><td>The number of valid EAPOL frames of any type that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Response ID</b></td><td>dot1xAuthEapolRespIdFramesRx</td><td>The number of valid EAP Resp/ID frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Responses</b></td><td>dot1xAuthEapolRespFramesRx</td><td>The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Start</b></td><td>dot1xAuthEapolStartFramesRx</td><td>The number of EAPOL Start frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Logoff</b></td><td>dot1xAuthEapolLogoffFramesRx</td><td>The number of valid EAPOL logoff frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Invalid Type</b></td><td>dot1xAuthInvalidEapolFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td></tr>
<tr><td>Rx</td><td><b>Invalid Length</b></td><td>dot1xAuthEapLengthErrorFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.</td></tr>
<tr><td>Tx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesTx</td><td>The number of EAPOL frames of any type that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Request ID</b></td><td>dot1xAuthEapolReqIdFramesTx</td><td>The number of EAP initial request frames that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Requests</b></td><td>dot1xAuthEapolReqFramesTx</td><td>The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.</td></tr>
</table></td></tr>
<tr><td>Backend Server Counters</td><td>Backend server frame counter statistics.
For MAC-based ports there are two tables containing backend server counters. The left-most shows a summary of all backend server counters on this port. The right-most shows backend server counters</td></tr>
</table>

<table>
<tr>
<td></td>
<td>for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables.
There are slight differences in the interpretation of the counters between port- and MAC-based authentication as shown below.

<table>
<tr><th colspan="4">Backend Server Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Access Challenges</b></td><td>dot1xAuthBackendAccessChallenges</td><td><b>Port-based</b>:
Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.
<b>MAC-based</b>:
Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</td></tr>
<tr><td>Rx</td><td><b>Other Requests</b></td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td><b>Port-based</b>:
Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td>Rx</td><td><b>Auth. Successes</b></td><td>dot1xAuthBackendAuthSuccesses</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</td></tr>
<tr><td>Rx</td><td><b>Auth. Failures</b></td><td>dot1xAuthBackendAuthFails</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</td></tr>
<tr><td>Tx</td><td><b>Responses</b></td><td>dot1xAuthBackendResponses</td><td><b>Port-based:</b>
Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
<b>MAC-based:</b>
Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Last Supplicant/Client Info</td>
<td>For MAC-based ports, this section is embedded in the backend server counter's section.
Information about the last supplicant/client that attempted to authenticate.

<table>
<tr><th colspan="3">Last Supplicant/Client Info</th></tr>
<tr><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td><b>Version</b></td><td>dot1xAuthLastEapolFrameVersion</td><td><b>Port-based</b>:
The protocol version number carried in the most recently received EAPOL frame.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td><b>Source</b></td><td>dot1xAuthLastEapolFrameSource</td><td><b>Port-based</b>:
The source MAC address carried in the most recently received EAPOL frame.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td><b>Identity or (Last) Client</b></td><td>-</td><td><b>Port-based</b>:
The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame.
<b>MAC-based</b>:
The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).</td></tr>
</table>
</td>
</tr>
<tr>
<td>Clients attached to this port</td>
<td>This table is only available for MAC-based ports
Each row in the table represents a MAC-based client on the port, and there are three parameters for each client:
MAC Address:
Shows the MAC address of the client, which is also used as the</td>
</tr>
</table>

	password in the authentication process against the backend server. Clicking the link causes the client's backend server counters to be shown in the right-most backend server counters table above. If no clients are attached, it shows No clients attached. State: Shows whether the client is authorized or unauthorized. As long as the backend server hasn't successfully authenticated a client, it is unauthorized. Last Authentication: Show the date and time of the last authentication of the client. This gets updated for every re-authentication of the client.



Authentication Configuration

Client Configuration

Client	Authentication Method	Fallback
telnet	local	□
ssh	local	□
web	local	□
console	local	□

RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address	Port	Secret
1	□		1813	
2	□		1813	
3	□		1813	
4	□		1813	

Client Configuration

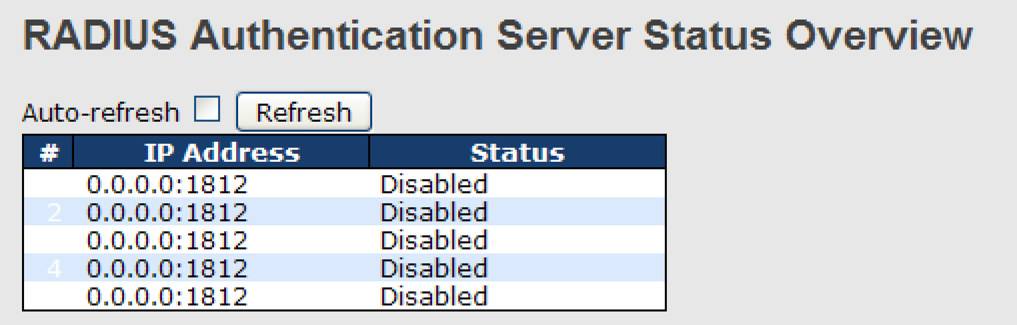
The table has one row for each Client and a number of columns, which are:

Label	Description
Client	The Client for which the configuration below applies.
Authentication Metohd	Authentication Method can be set to one of the following values: none : authentication is disabled and login is not possible. local : use the local user database on the switch stack for authentication. radius : use a remote RADIUS server for authentication. tacacs+ : use a remote TACACS+ server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enable	Enable the RADIUS Authentication Server by checking this box.
IP Address	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.

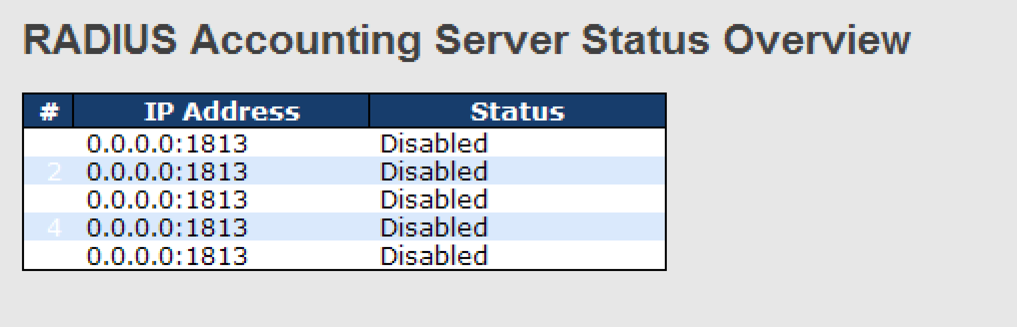


RADIUS Authentication Server Status Overview

Auto-refresh □ Refresh

#	IP Address	Status
	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
	0.0.0.0:1812	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.



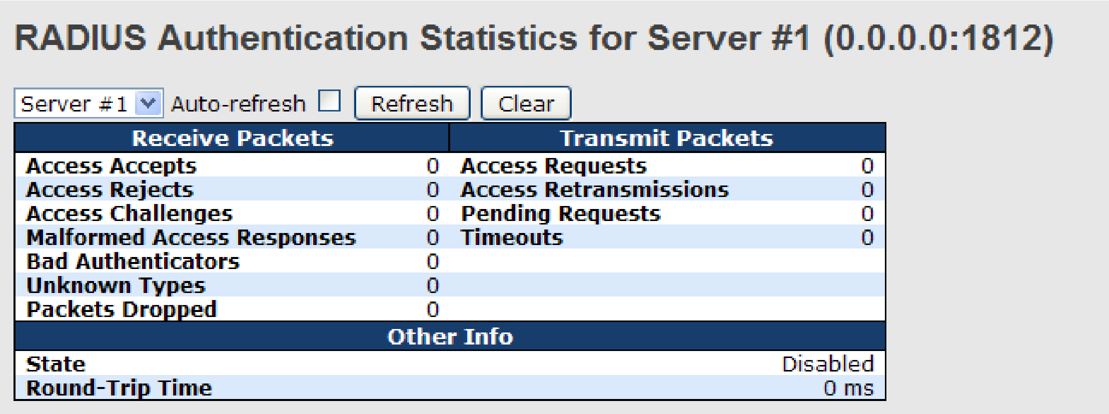
RADIUS Accounting Server Status Overview

#	IP Address	Status
	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
	0.0.0.0:1813	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed

	statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

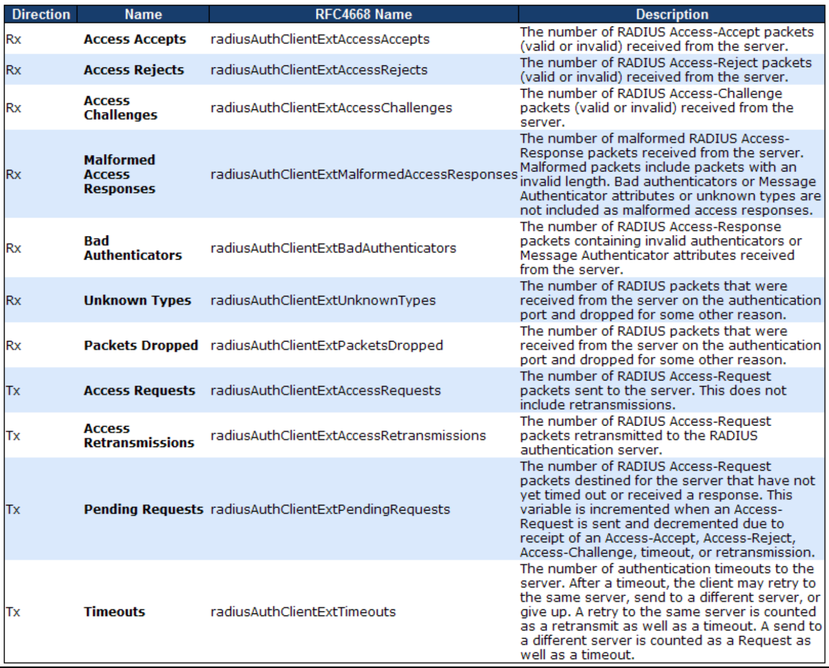


RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

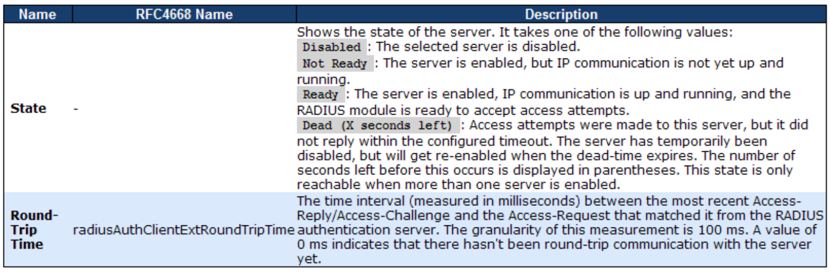
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
State	Disabled
Round-Trip Time	0 ms

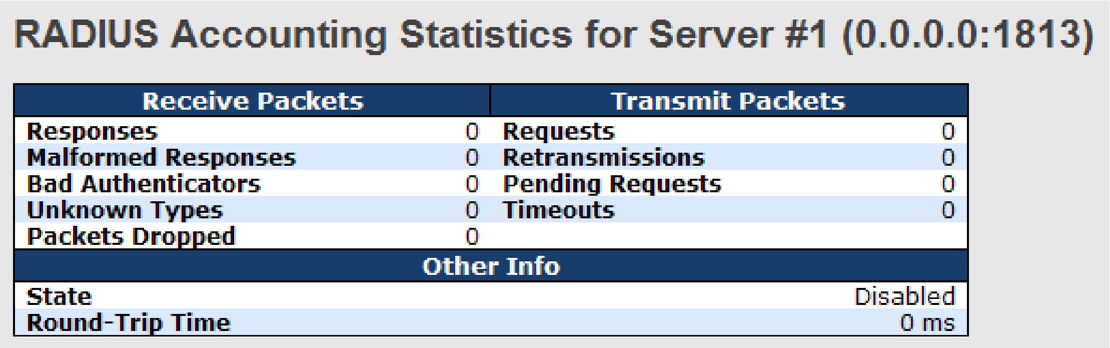
Label	Description
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info	This section contains information about the state of the server and the latest round-trip time. 

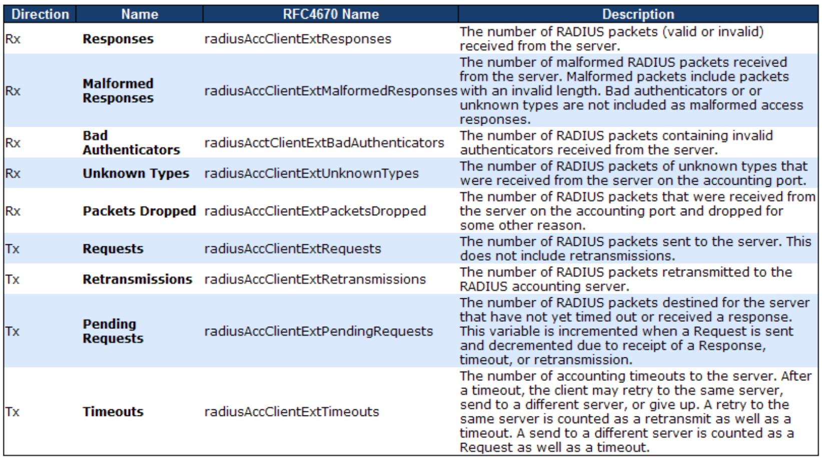
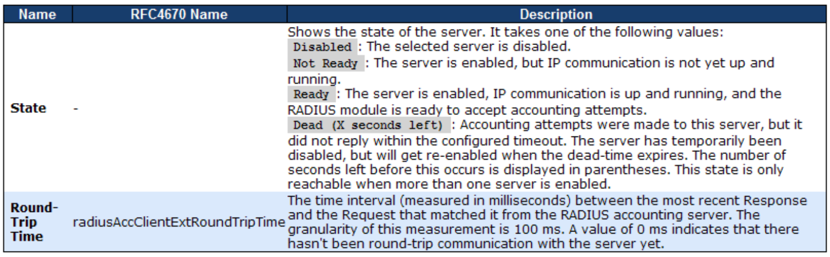
Name	RFC4668 Name	Description
State	-	Shows the state of the server. It takes one of the following values: `Disabled`: The selected server is disabled. `Not Ready`: The server is enabled, but IP communication is not yet up and running. `Ready`: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. `Dead (X seconds left)`: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.



RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	**Requests**	0
Malformed Responses	0	**Retransmissions**	0
Bad Authenticators	0	**Pending Requests**	0
Unknown Types	0	**Timeouts**	0
Packets Dropped	0		
Other Info			
State			Disabled
Round-Trip Time			0 ms

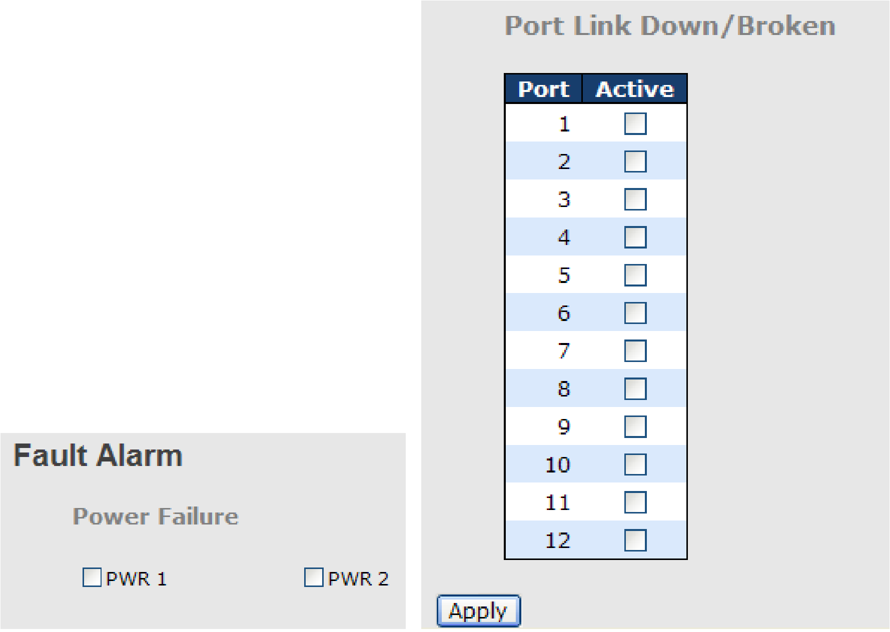
Label	Description
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.

<table>
<tr>
<td></td>
<td>

<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Responses</b></td><td>radiusAccClientExtResponses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td><b>Malformed Responses</b></td><td>radiusAccClientExtMalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td><b>Bad Authenticators</b></td><td>radiusAcctClientExtBadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr>
<tr><td>Rx</td><td><b>Unknown Types</b></td><td>radiusAccClientExtUnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr>
<tr><td>Rx</td><td><b>Packets Dropped</b></td><td>radiusAccClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td><b>Requests</b></td><td>radiusAccClientExtRequests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td><b>Retransmissions</b></td><td>radiusAccClientExtRetransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr>
<tr><td>Tx</td><td><b>Pending Requests</b></td><td>radiusAccClientExtPendingRequests</td><td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td><b>Timeouts</b></td><td>radiusAccClientExtTimeouts</td><td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Other Info</td>
<td>
This section contains information about the state of the server and the latest

<table>
<tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td><b>State</b></td><td>-</td><td>Shows the state of the server. It takes one of the following values:
Disabled : The selected server is disabled.
Not Ready : The server is enabled, but IP communication is not yet up and running.
Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
Dead (X seconds left) : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr>
<tr><td><b>Round-Trip Time</b></td><td>radiusAccClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr>
</table>
</td>
</tr>
</table>

5.1.11 Warning

5.1.11.1 Fault Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.



Fault Alarm

Power Failure

□ PWR 1 □ PWR 2

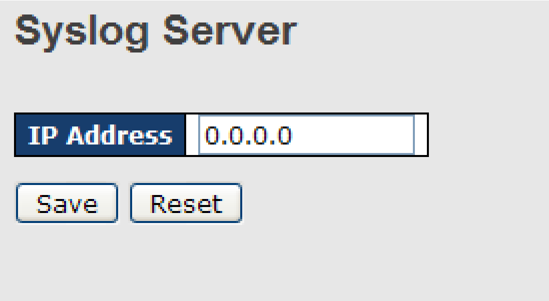
Port Link Down/Broken

Port	Active
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□
11	□
12	□

5.1.11.2 System Warning

5.1.11.2.1 SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol



Syslog Server

IP Address	0.0.0.0

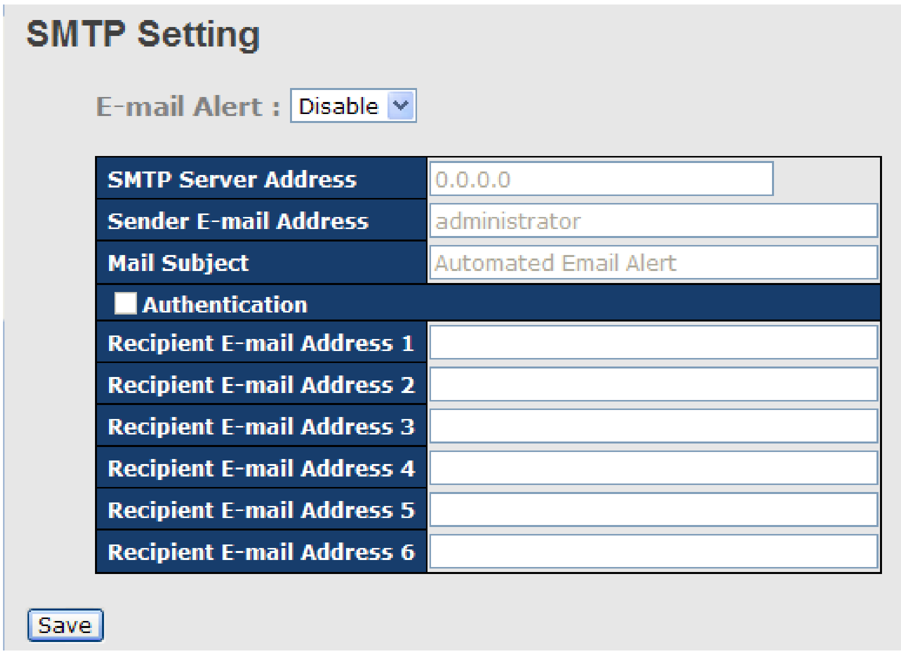
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
SYSLOG Server IP Address	The remote SYSLOG Server IP address.

5.1.11.2.2 SMTP Setting

The SMTP is Short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.



SMTP Setting

E-mail Alert : Disable

SMTP Server Address	0.0.0.0
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
□ Authentication	
Recipient E-mail Address 1	
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

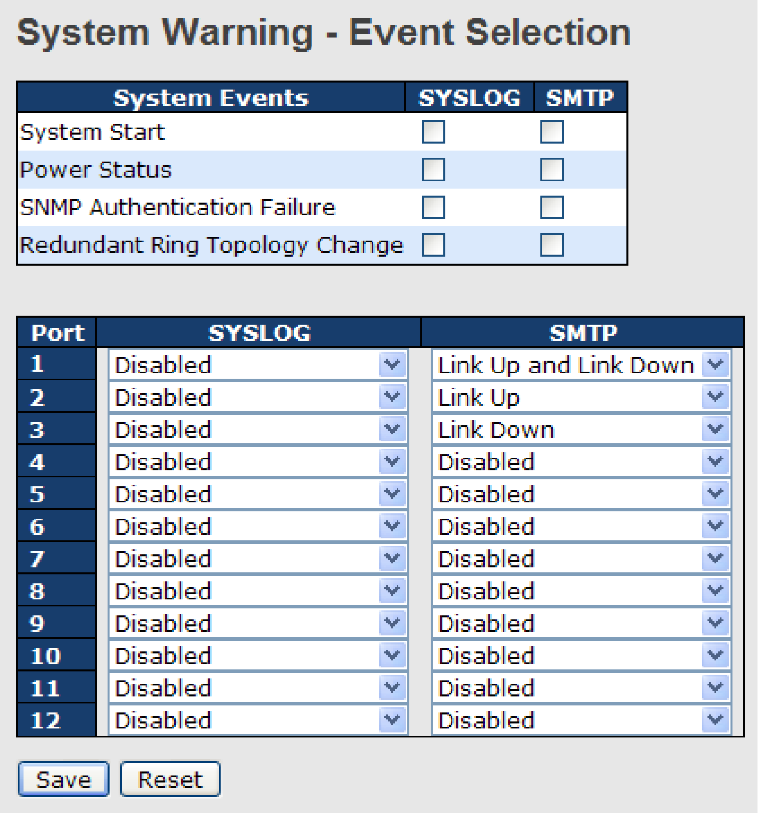
System Warning – SMTP Setting interface

The following table describes the labels in this screen.

Label	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	The SMTP server IP address
Mail Subject	The Subject of the mail
Authentication	■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.11.2.3 Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.



System Warning - Event Selection

System Events	SYSLOG	SMTP
System Start	□	□
Power Status	□	□
SNMP Authentication Failure	□	□
Redundant Ring Topology Change	□	□

Port	SYSLOG	SMTP
1	Disabled	Link Up and Link Down
2	Disabled	Link Up
3	Disabled	Link Down
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled

System Warning – Event Selection interface

The following table describes the labels in this screen.

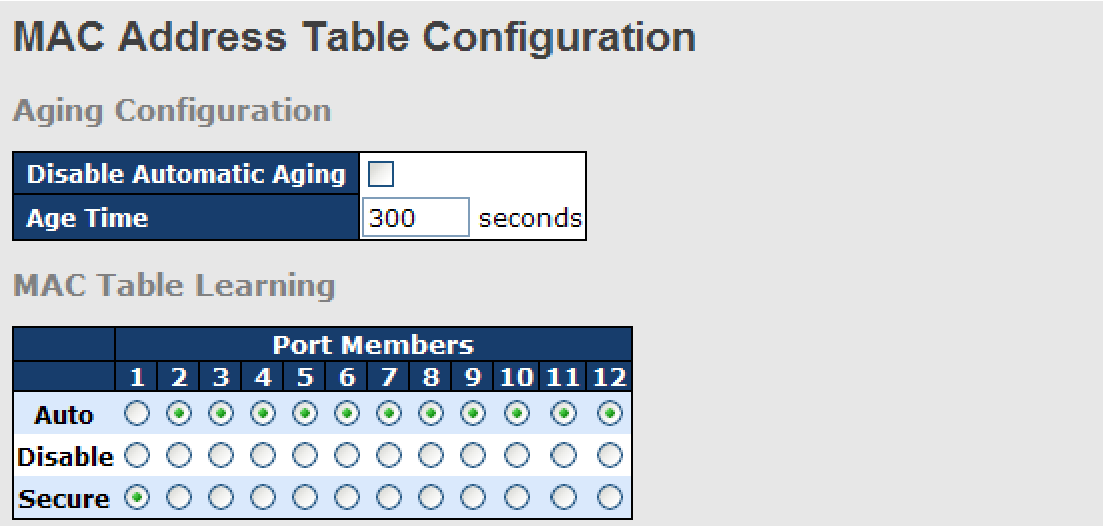
Label	Description
System Event	
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
O-Ring Topology Change	Alert when O-Ring topology changes.
Port Event **SYSLOG / SMTP event**	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.12 Monitor and Diag

5.1.12.1 MAC Table

5.1.12.1.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.



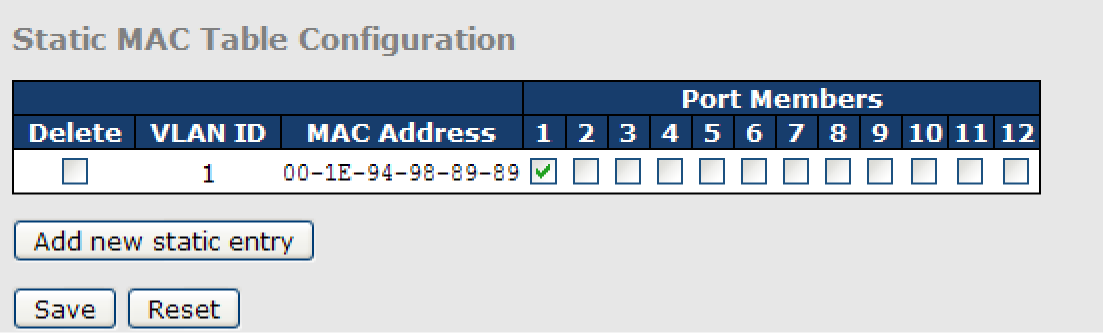
MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Age Time	300 seconds

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	○	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○
Secure	●	○	○	○	○	○	○	○	○	○	○	○



Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
□	1	00-1E-94-98-89-89	☑	□	□	□	□	□	□	□	□	□	□	□

Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** ▭ seconds.

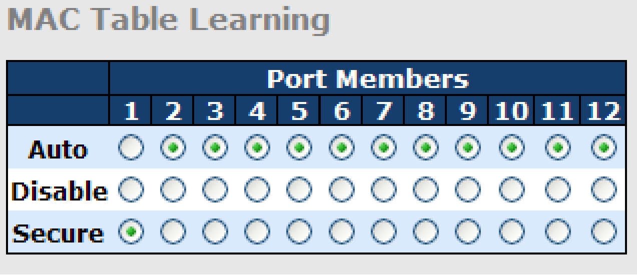
The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking □ **Disable automatic aging**.

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:



MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	○	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○
Secure	●	○	○	○	○	○	○	○	○	○	○	○

Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning

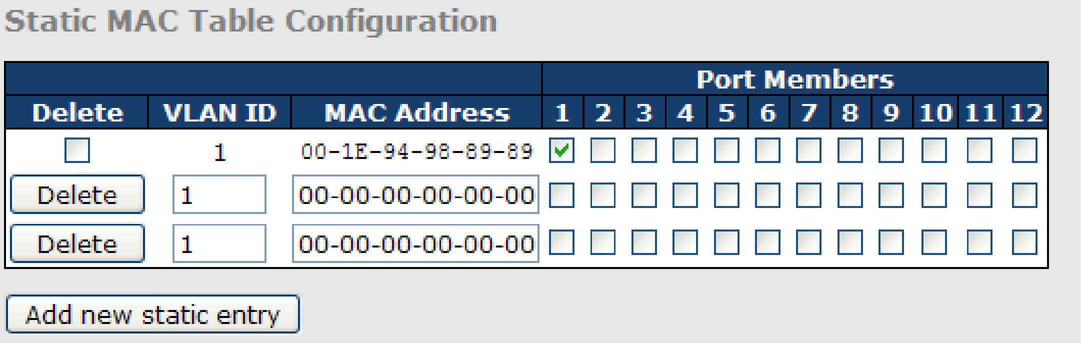
	mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.



Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
☐	1	00-1E-94-98-89-89	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add new static entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

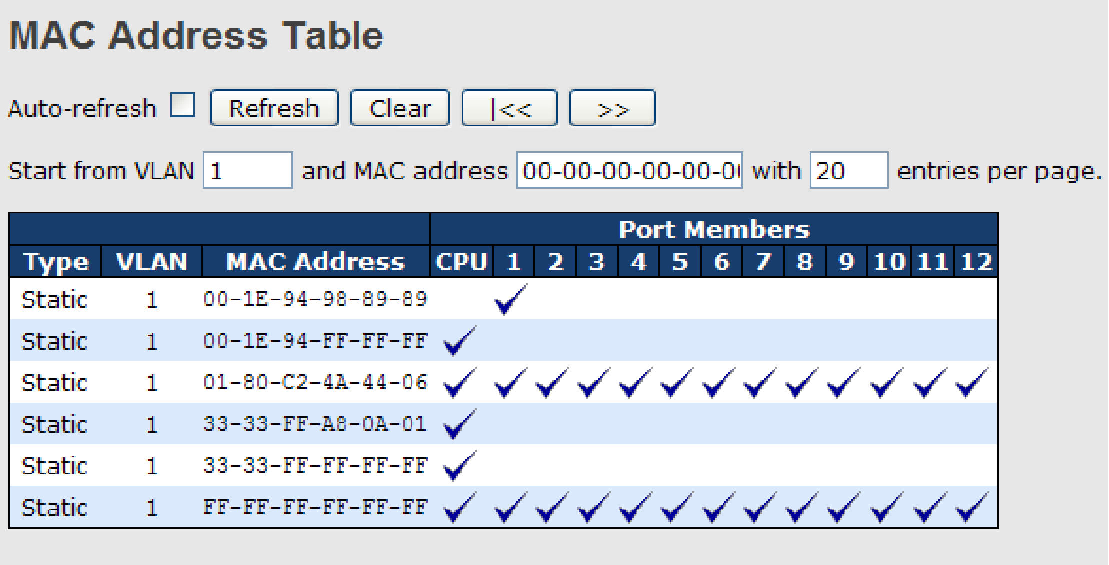
5.1.12.1.2 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will -

upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the |<< button to start over.



MAC Address Table

Auto-refresh □ Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-0(with 20 entries per page.

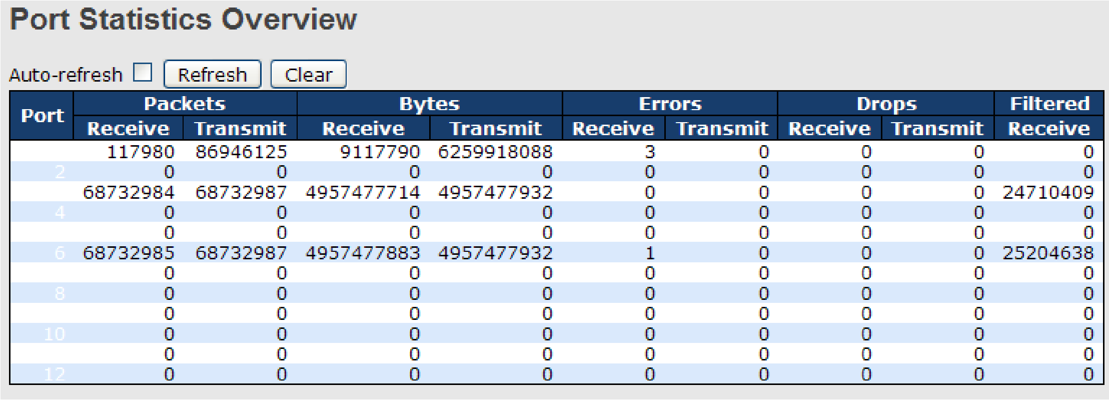
			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Static	1	00-1E-94-98-89-89		✓											
Static	1	00-1E-94-FF-FF-FF	✓												
Static	1	01-80-C2-4A-44-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-A8-0A-01	✓												
Static	1	33-33-FF-FF-FF-FF	✓												
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

5.1.12.2 Port Statistic

5.1.12.2.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.



Port Statistics Overview

Auto-refresh □ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
	117980	86946125	9117790	6259918088	3	0	0	0	0
2	0	0	0	0	0	0	0	0	0
	68732984	68732987	4957477714	4957477932	0	0	0	0	24710409
4	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
6	68732985	68732987	4957477883	4957477932	1	0	0	0	25204638
	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

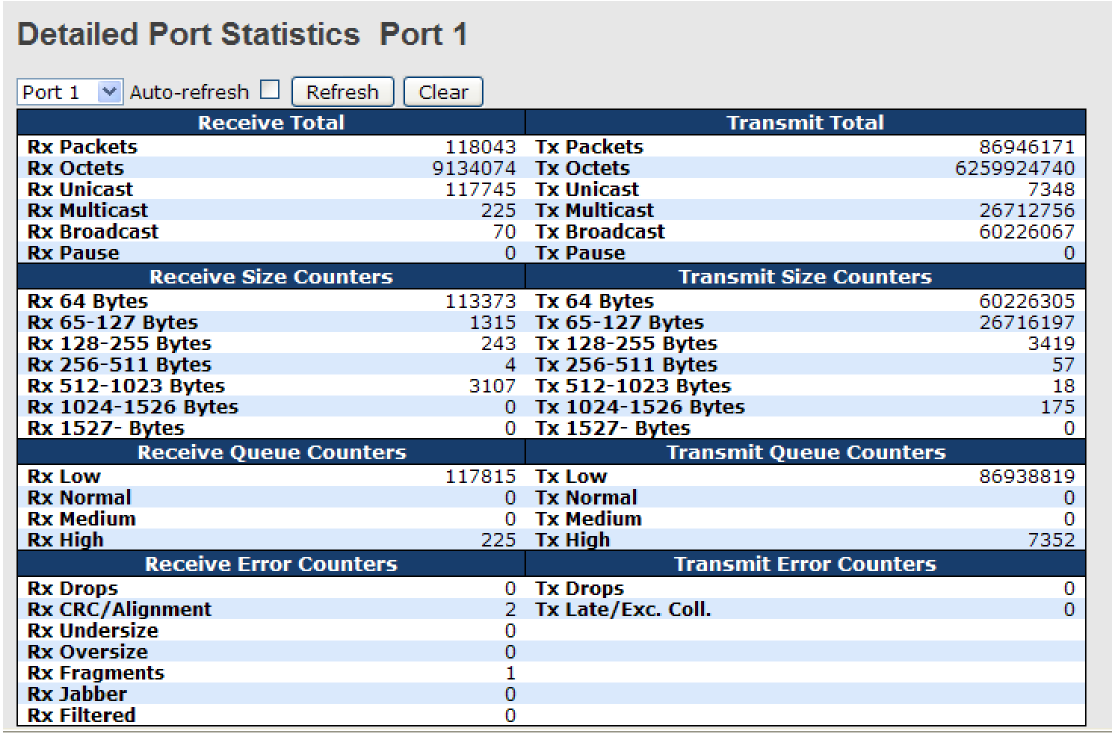
Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the counters entries, starting from the current entry ID.
Clear	Flushes all counters entries.

5.1.12.2.2 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Statistics-Receive & Transmit Total



Detailed Port Statistics Port 1

Port 1 ▾ Auto-refresh □ Refresh Clear

Receive Total		Transmit Total	
Rx Packets	118043	Tx Packets	86946171
Rx Octets	9134074	Tx Octets	6259924740
Rx Unicast	117745	Tx Unicast	7348
Rx Multicast	225	Tx Multicast	26712756
Rx Broadcast	70	Tx Broadcast	60226067
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	113373	Tx 64 Bytes	60226305
Rx 65-127 Bytes	1315	Tx 65-127 Bytes	26716197
Rx 128-255 Bytes	243	Tx 128-255 Bytes	3419
Rx 256-511 Bytes	4	Tx 256-511 Bytes	57
Rx 512-1023 Bytes	3107	Tx 512-1023 Bytes	18
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	175
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Low	117815	Tx Low	86938819
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	225	Tx High	7352
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	2	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	1		
Rx Jabber	0		
Rx Filtered	0		

Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.

Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

5.1.12.3 Port Mirroring

Configure port Mirroring on this page.

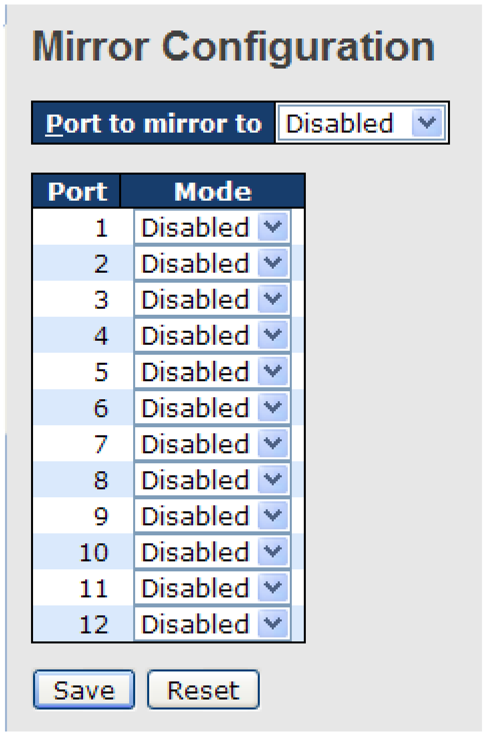
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror also knwon as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.



Mirror Configuration

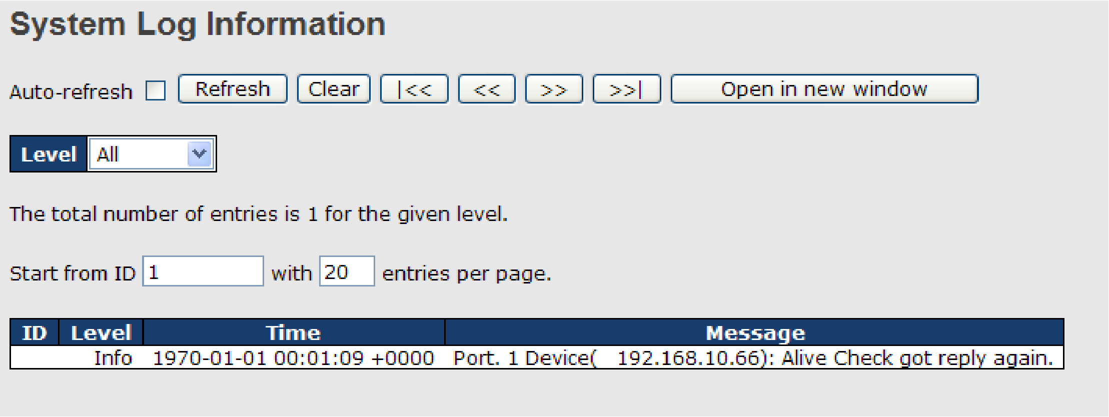
Port to mirror to: Disabled

Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled

Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. Rx only : Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only :Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled : Neither frames transmitted nor frames received are mirrored. Enabled : Frames received and frames transmitted are mirrored to the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

5.1.12.4 System Log Information

The switch system log information is provided here.



System Log Information

Auto-refresh ☐

Level: All

The total number of entries is 1 for the given level.

Start from ID 1 with 20 entries per page.

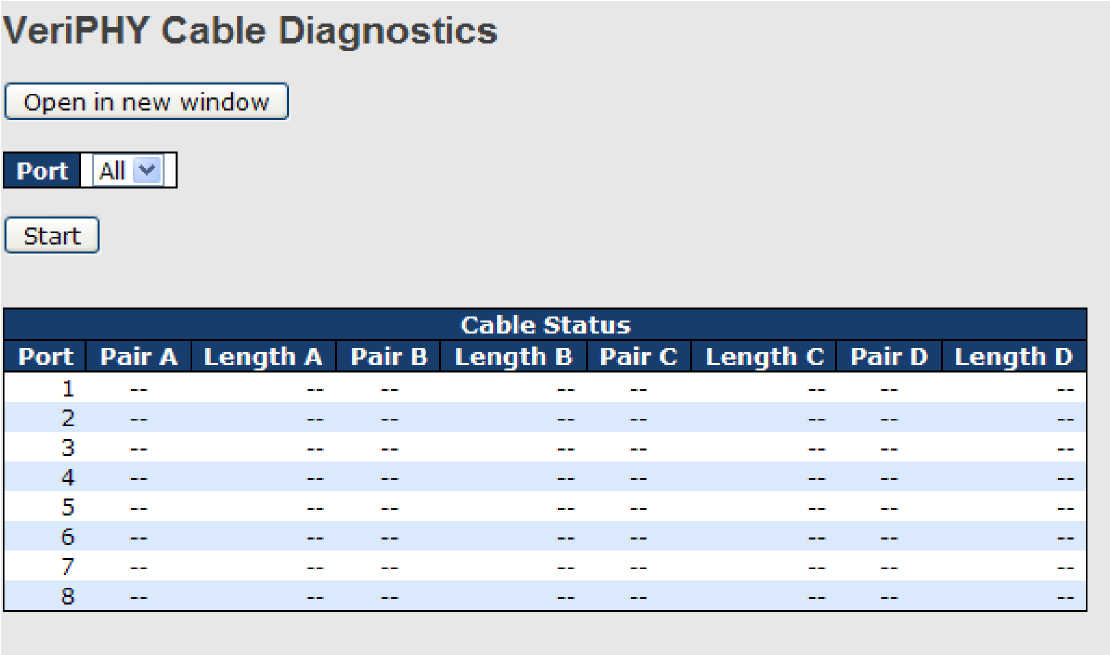
ID	Level	Time	Message
	Info	1970-01-01 00:01:09 +0000	Port. 1 Device(192.168.10.66): Alive Check got reply again.

Label	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log.

	Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
|<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>|	Updates the system log entries, ending at the last available entry ID.

5.1.12.5 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.



VeriPHY Cable Diagnostics

Open in new window

Port: All

Start

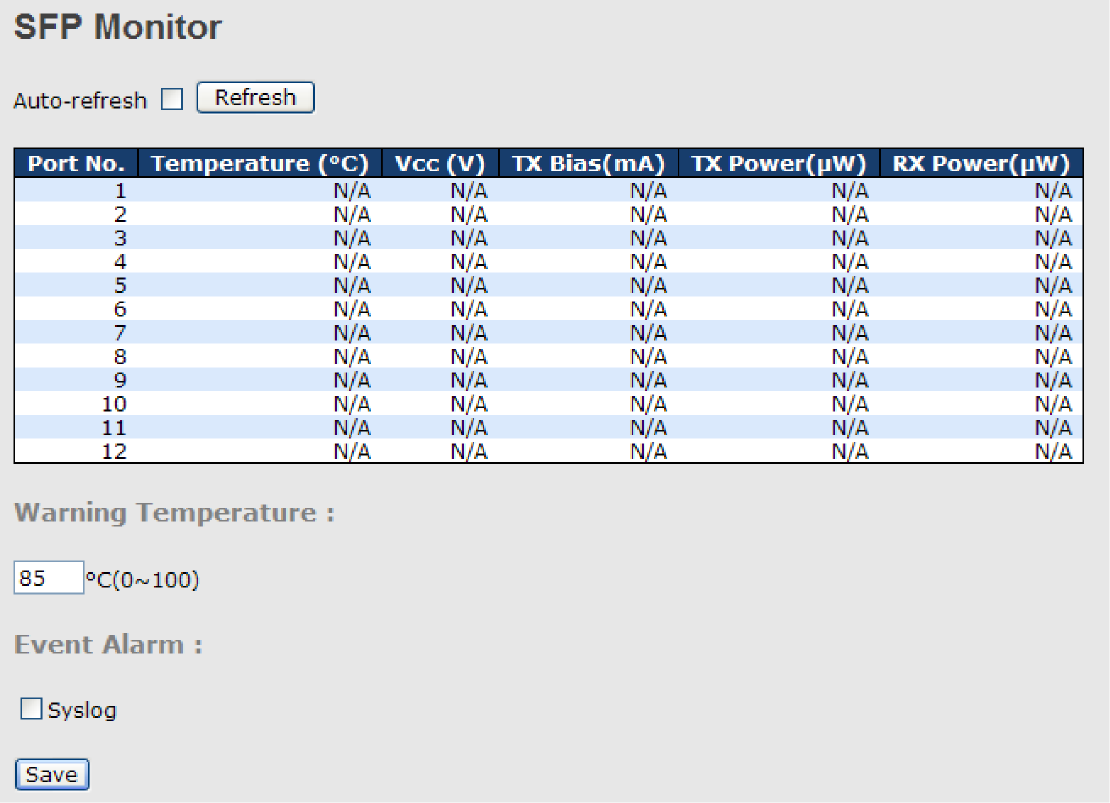
Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

Press Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

5.1.12.6 SFP Monitor

DDM function, can pass SFP module which supports DDM function, measure the temperature of the apparatus .And manage and set up event alarm module through DDM WEB



SFP Monitor

Auto-refresh □ Refresh

Port No.	Temperature (°C)	Vcc (V)	TX Bias(mA)	TX Power(μW)	RX Power(μW)
1	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

85 °C(0~100)

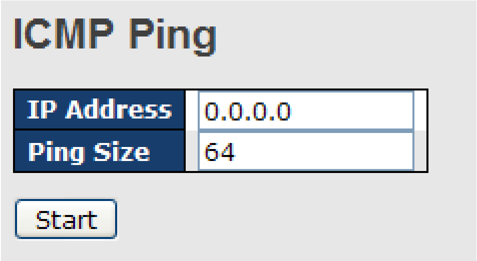
Event Alarm :

□ Syslog

Save

5.1.12.7 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



ICMP Ping

IP Address	0.0.0.0
Ping Size	64

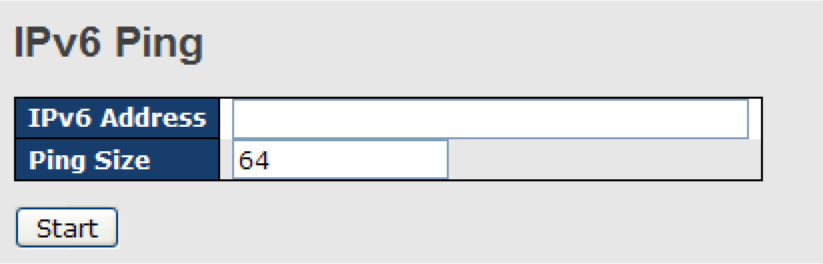
After you press Start, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

5.1.12.8 IPv6 Ping



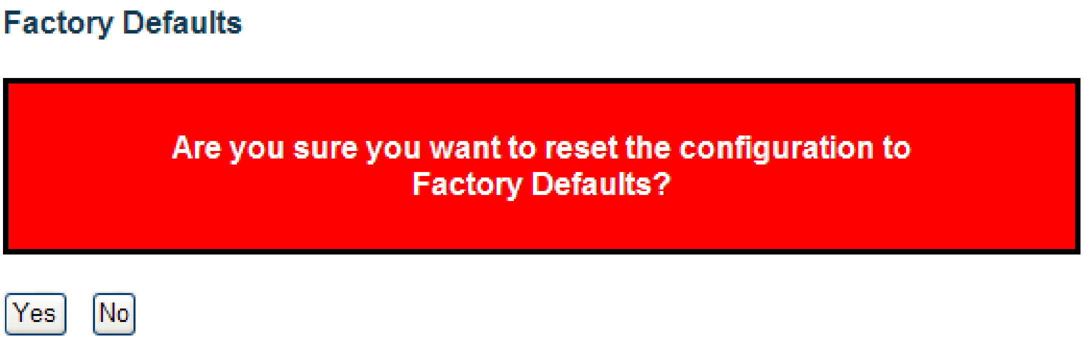
IPv6 Ping

IPv6 Address	
Ping Size	64

```
PING6 server ::192.168.10.1
sendto
sendto
sendto
sendto
sendto
Sent 5 packets, received 0 OK, 0 bad
```

5.1.13 Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.



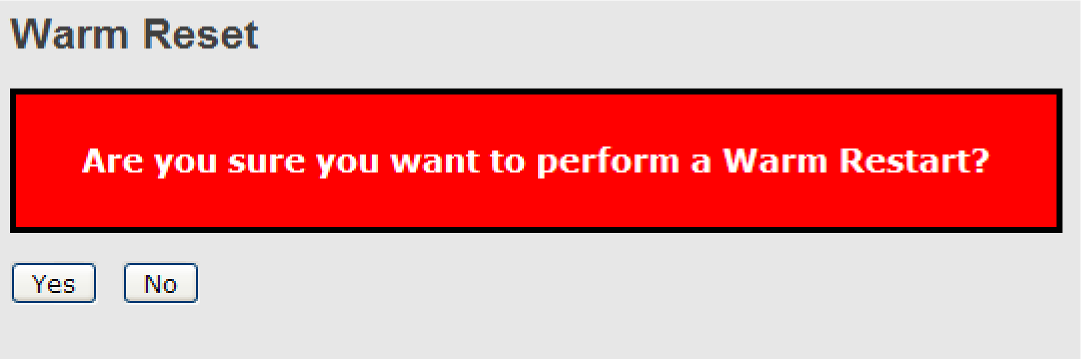
Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration

5.1.14 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices



Warm Reset

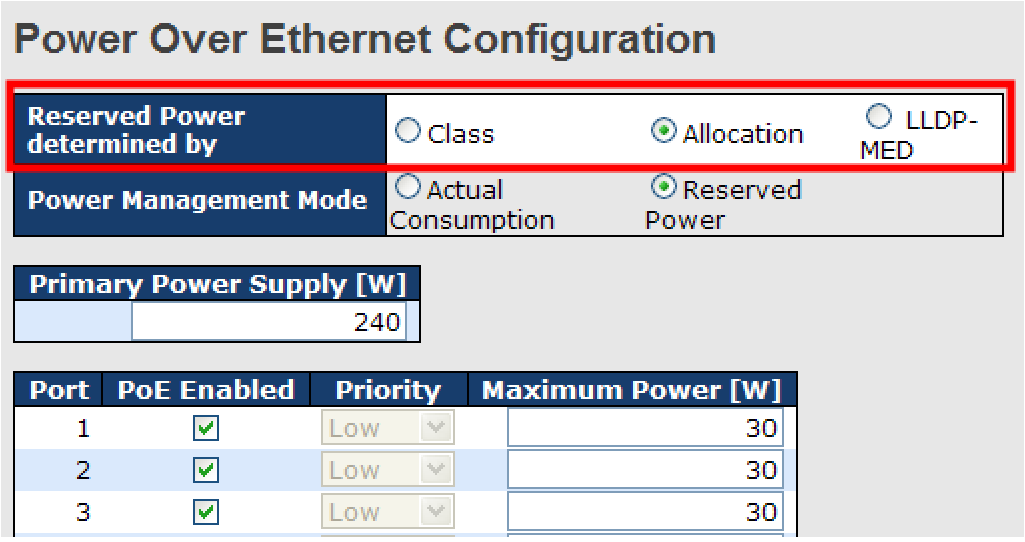
Are you sure you want to perform a Warm Restart?

Label	Description
Yes	Click to reboot device.
No	Click to return to the Port State page without rebooting.

5.1.15 Power Over Ethernet

5.1.15.1 PoE Configuration - Reserved Power determined

There are three modes for configuring how the ports/PDs may reserve power.



Power Over Ethernet Configuration

Reserved Power determined by	○ Class ● Allocation ○ LLDP-MED
Power Management Mode	○ Actual Consumption ● Reserved Power

Primary Power Supply [W]
240

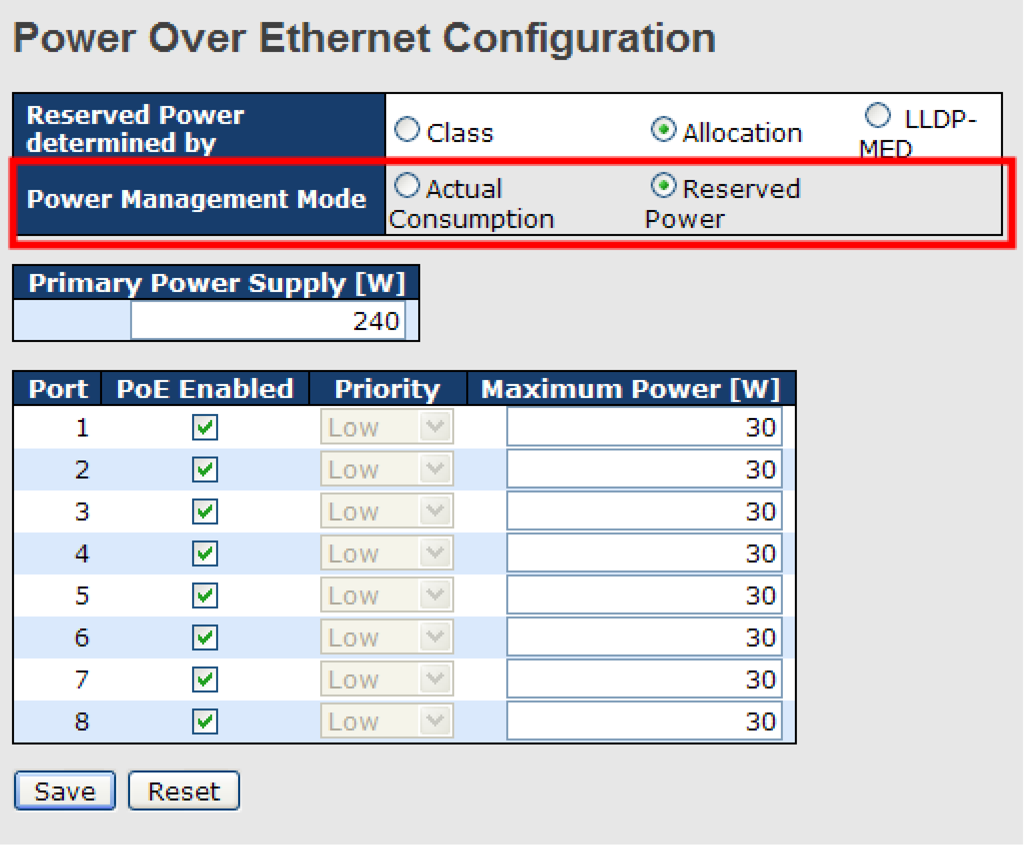
Port	PoE Enabled	Priority	Maximum Power [W]
1	☑	Low	30
2	☑	Low	30
3	☑	Low	30

Label	Description
Allocated mode	In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
Class mode	In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Three different port classes exist and one for 4, 7 and 15.4 Watts. (In this mode the Maximum Power fields have no effect.)
LLDP-MED mode	This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode.(In this mode the Maximum Power fields have no effect)

(For all mode : If a port uses more power than the reserved power for the port, the port is shut down.)

5.1.15.2 PoE Configuration - Power management Mode

There are 2 modes for configuring when to the ports are shut down.



Power Over Ethernet Configuration

Reserved Power determined by	○ Class	● Allocation	○ LLDP-MED
Power Management Mode	○ Actual Consumption	● Reserved Power	

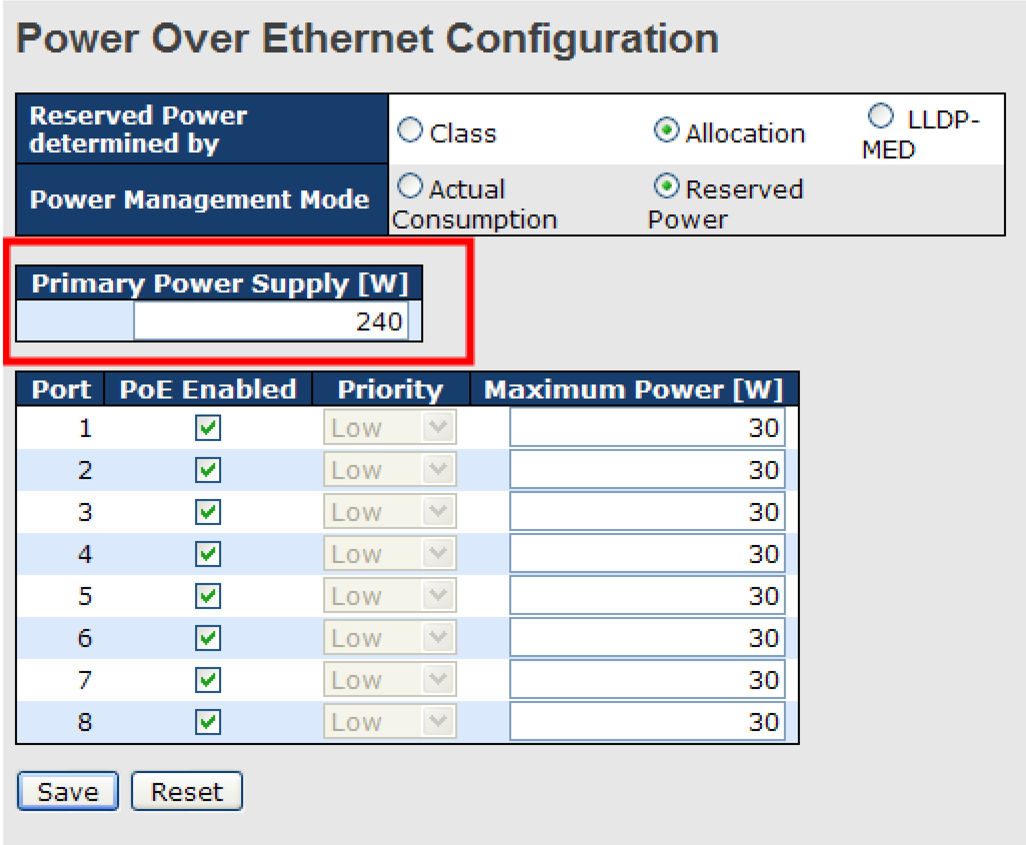
Primary Power Supply [W]
240

Port	PoE Enabled	Priority	Maximum Power [W]
1	☑	Low	30
2	☑	Low	30
3	☑	Low	30
4	☑	Low	30
5	☑	Low	30
6	☑	Low	30
7	☑	Low	30
8	☑	Low	30

Label	Description
Actual Consumption	In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
Reserved Power	In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power the available.

5.1.15.3 PoE Configuration - Primary Power Supply

primary power source, user can setting maximum input power range.



Power Over Ethernet Configuration

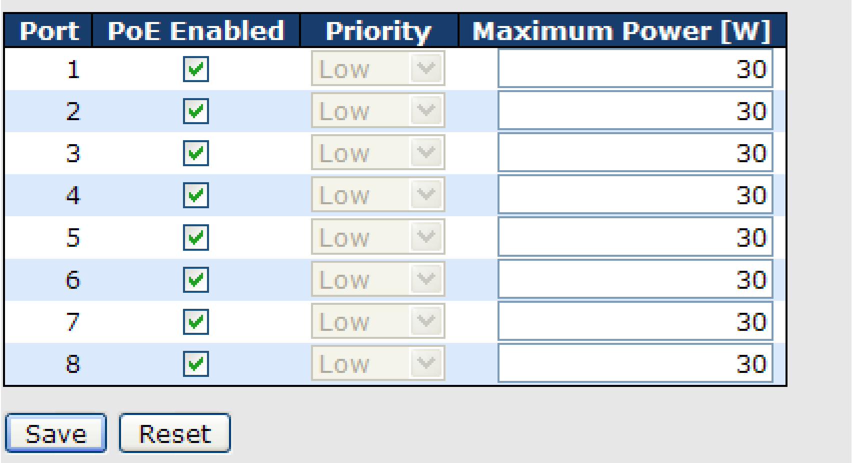
Reserved Power determined by	○ Class	● Allocation	○ LLDP-MED
Power Management Mode	○ Actual Consumption	● Reserved Power	

Primary Power Supply [W]
240

Port	PoE Enabled	Priority	Maximum Power [W]
1	☑	Low	30
2	☑	Low	30
3	☑	Low	30
4	☑	Low	30
5	☑	Low	30
6	☑	Low	30
7	☑	Low	30
8	☑	Low	30

5.1.15.4 PoE Configuration - Port Configuration

User can configuration every port PoE Setting

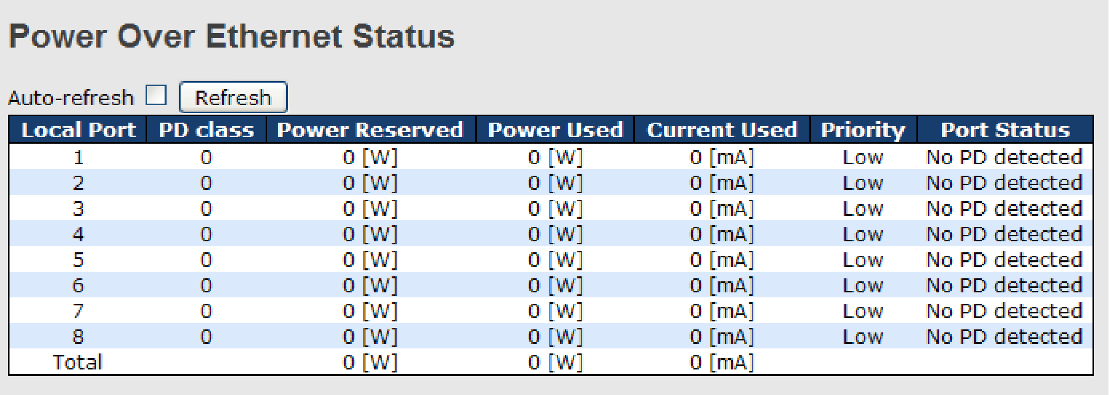


Port	PoE Enabled	Priority	Maximum Power [W]
1	☑	Low	30
2	☑	Low	30
3	☑	Low	30
4	☑	Low	30
5	☑	Low	30
6	☑	Low	30
7	☑	Low	30
8	☑	Low	30

Label	Description
PoE Enable	The PoE Enabled represents whether the PoE is enable for the port.
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices requires uses more power than power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the lowest port number.
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delived to a remote device.(The maximum allowed value is 102.3 W.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.15.5 Power over Ethernet Status

This page allows the user to inspect the current status for all PoE ports.



Power Over Ethernet Status

Auto-refresh □ Refresh

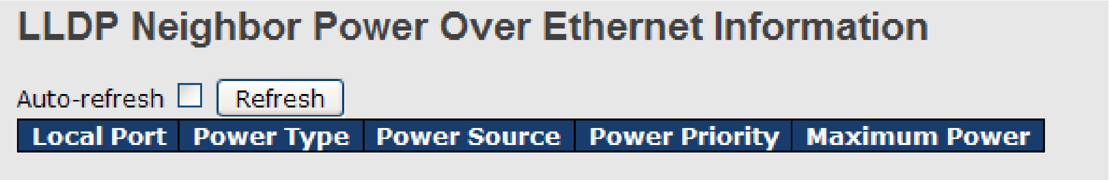
Local Port	PD class	Power Reserved	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [mA]		

Label	Description
Local Port	This is the logical port number for this row.
Power Reserved	The Power Reserved shows how much the power the PD has reserved.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is

	using. P.O.E. ports
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status.

5.1.15.6 LLDP Power Over Ethernet Neighbor

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information:



LLDP Neighbor Power Over Ethernet Information

Auto-refresh □ Refresh

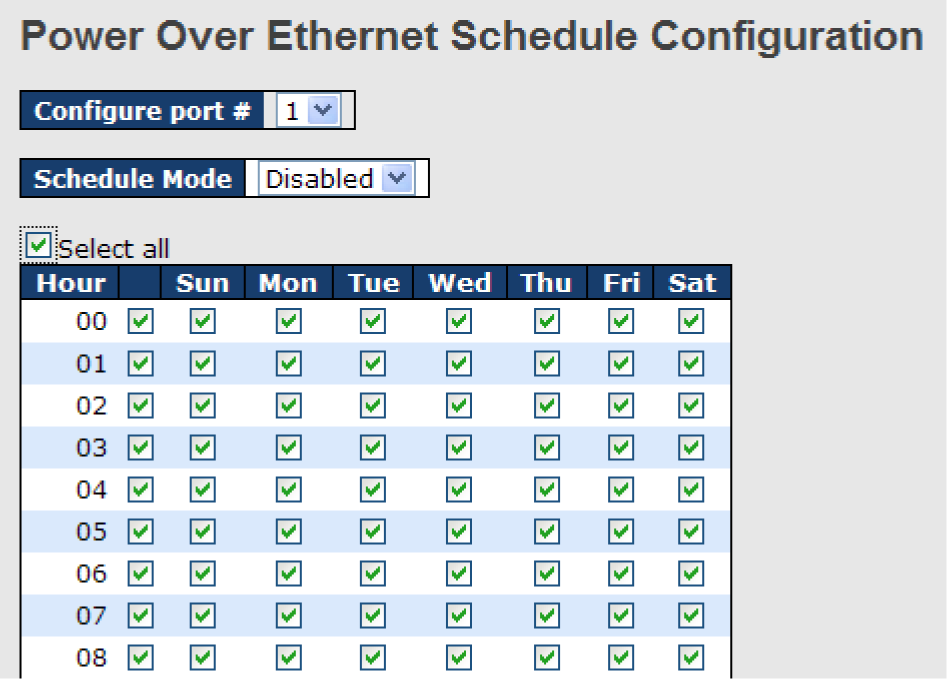
Local Port	Power Type	Power Source	Power Priority	Maximum Power

Label	Description
Local Port	The port for this switch on which the LLDP frame was received.
Power Type	The Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Type is unknown it is represented as "Resevered".
Power Source	The Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as "Unknown"
Power Priority	The Power Used shows how much current the PD currently is using. P.O.E. ports
Power Priority	Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The

	three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown"
Maximum Power	The Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"
Refresh	Click to refresh the page immediately.
Auto-refresh □	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.15.7 PoE Schedule

User can appointed date and time, Enable or Close Power Over Ethernet Function, switch can with according to the time when is set up, carry on the designated movements (SNTP Function must Enable)



Power Over Ethernet Schedule Configuration

Configure port # 1

Schedule Mode Disabled

☑ Select all

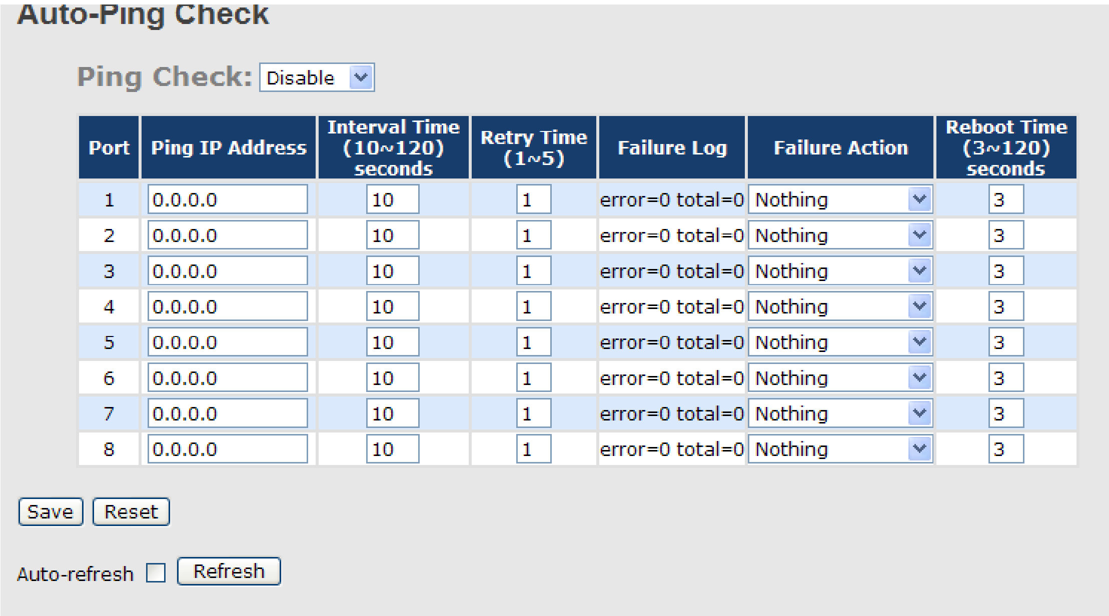
Hour		Sun	Mon	Tue	Wed	Thu	Fri	Sat
00	☑	☑	☑	☑	☑	☑	☑	☑
01	☑	☑	☑	☑	☑	☑	☑	☑
02	☑	☑	☑	☑	☑	☑	☑	☑
03	☑	☑	☑	☑	☑	☑	☑	☑
04	☑	☑	☑	☑	☑	☑	☑	☑
05	☑	☑	☑	☑	☑	☑	☑	☑
06	☑	☑	☑	☑	☑	☑	☑	☑
07	☑	☑	☑	☑	☑	☑	☑	☑
08	☑	☑	☑	☑	☑	☑	☑	☑

The following table describes the labels in this screen.

Label	Description
Configure port	Setting action port
Schedule mode	Schedule mode enable or disable
Select all	Select all Data & Time
Hour	Set up enable Time
Sunday~Saturday	Set up enable Data

5.1.15.8 Auto-Ping Check

You can control the POE function by using the ping command , in order to turn on or off other POE device which connect with port assign.



Auto-Ping Check

Ping Check: Disable

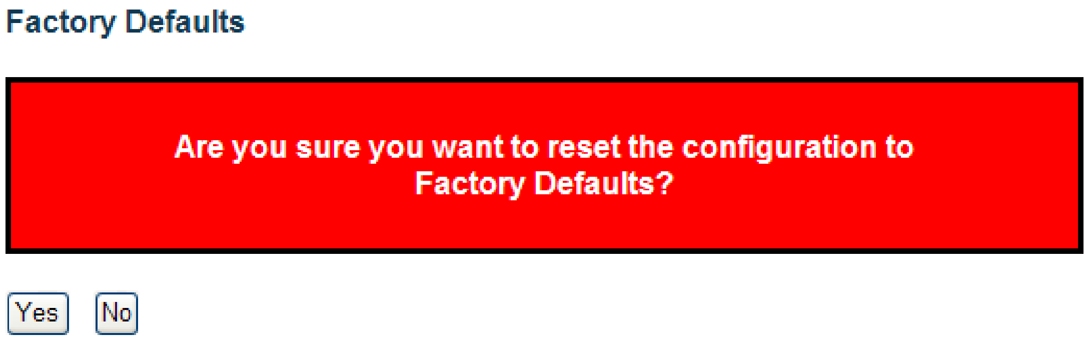
Port	Ping IP Address	Interval Time (10~120) seconds	Retry Time (1~5)	Failure Log	Failure Action	Reboot Time (3~120) seconds
1	0.0.0.0	10	1	error=0 total=0	Nothing	3
2	0.0.0.0	10	1	error=0 total=0	Nothing	3
3	0.0.0.0	10	1	error=0 total=0	Nothing	3
4	0.0.0.0	10	1	error=0 total=0	Nothing	3
5	0.0.0.0	10	1	error=0 total=0	Nothing	3
6	0.0.0.0	10	1	error=0 total=0	Nothing	3
7	0.0.0.0	10	1	error=0 total=0	Nothing	3
8	0.0.0.0	10	1	error=0 total=0	Nothing	3

The following table describes the labels in this screen.

Label	Description
Ping Check	Enable or disable Ping Check function
Port	You can appoint to want to control P.O.E port number
Ping IP Address	Set up ip Address
Interval Time	Spacing interval to set up Ping(10 Sec~120 Sec)
Retry Time	Set up the number of times of ping
Failure Log	Note down " Ping Check " a result of movement after starting.
Failure Action	Set up movements wanted to carry out
Reboot Time	Switch ping check failure " P.O.E " restarts the buffer time of switch.

5.1.16 Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.



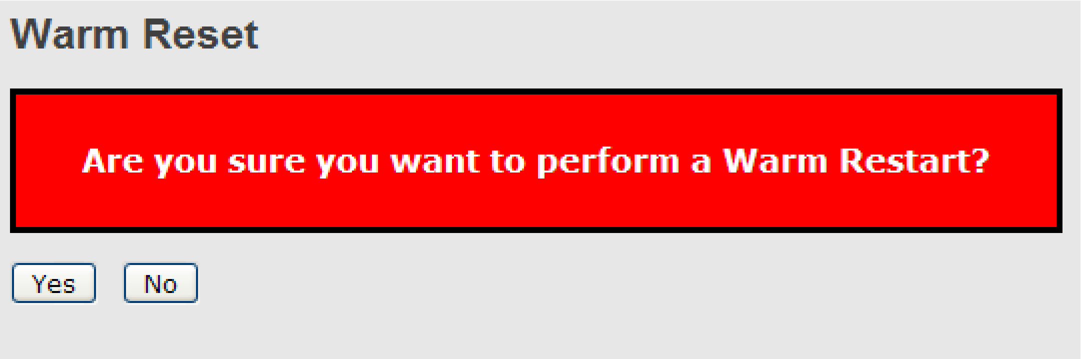
Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration

5.1.17 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices



Warm Reset

Are you sure you want to perform a Warm Restart?

Label	Description
Yes	Click to reboot device.
No	Click to return to the Port State page without rebooting.

Command Line Interface Management

6.1 About CLI Management

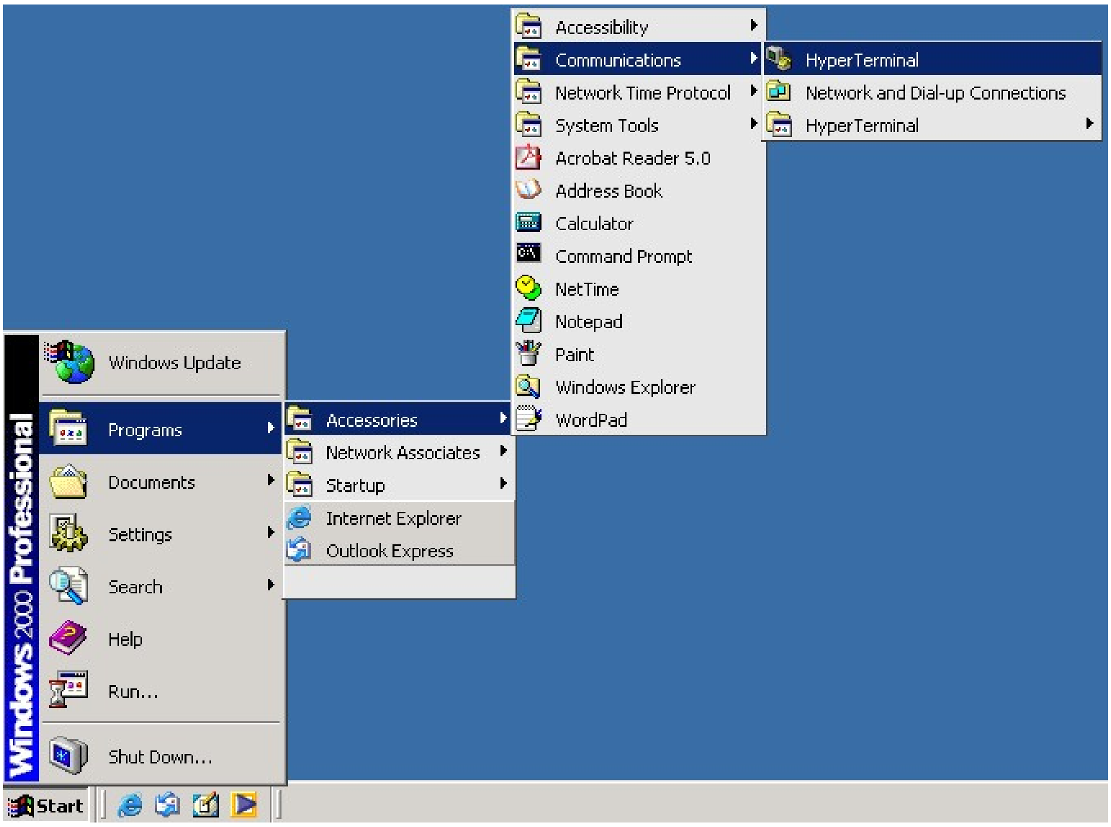
Besides WEB-base management, IES-3073GC also support CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

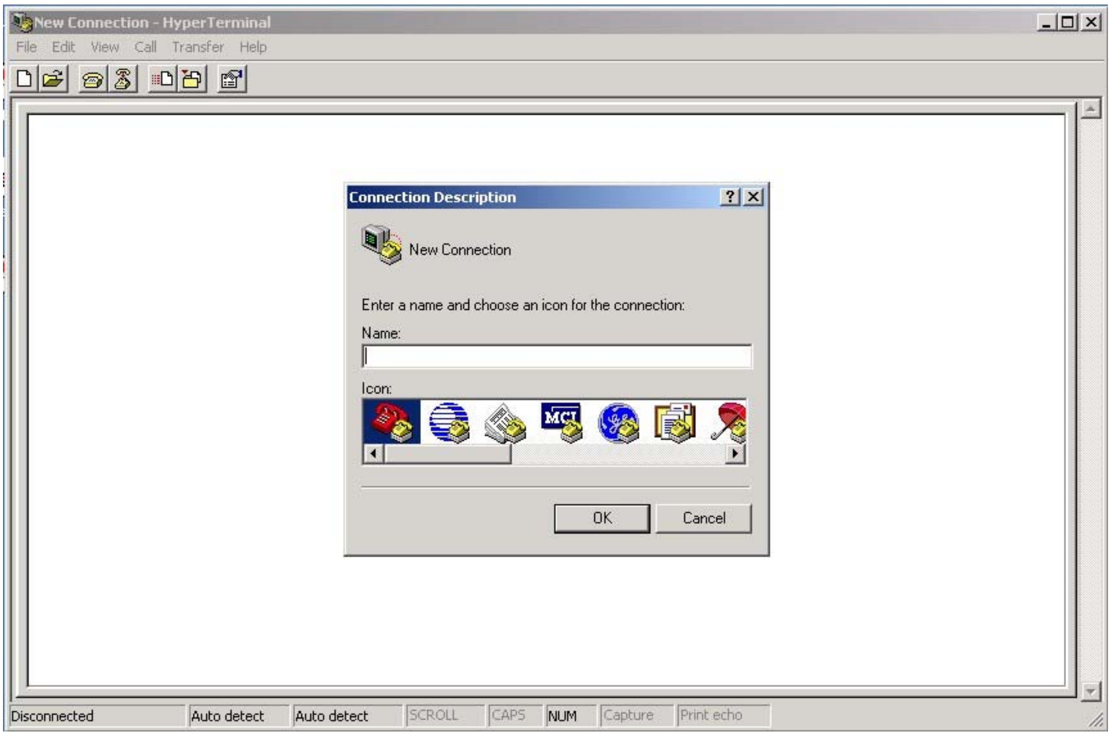
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



Step 2. Input a name for new connection

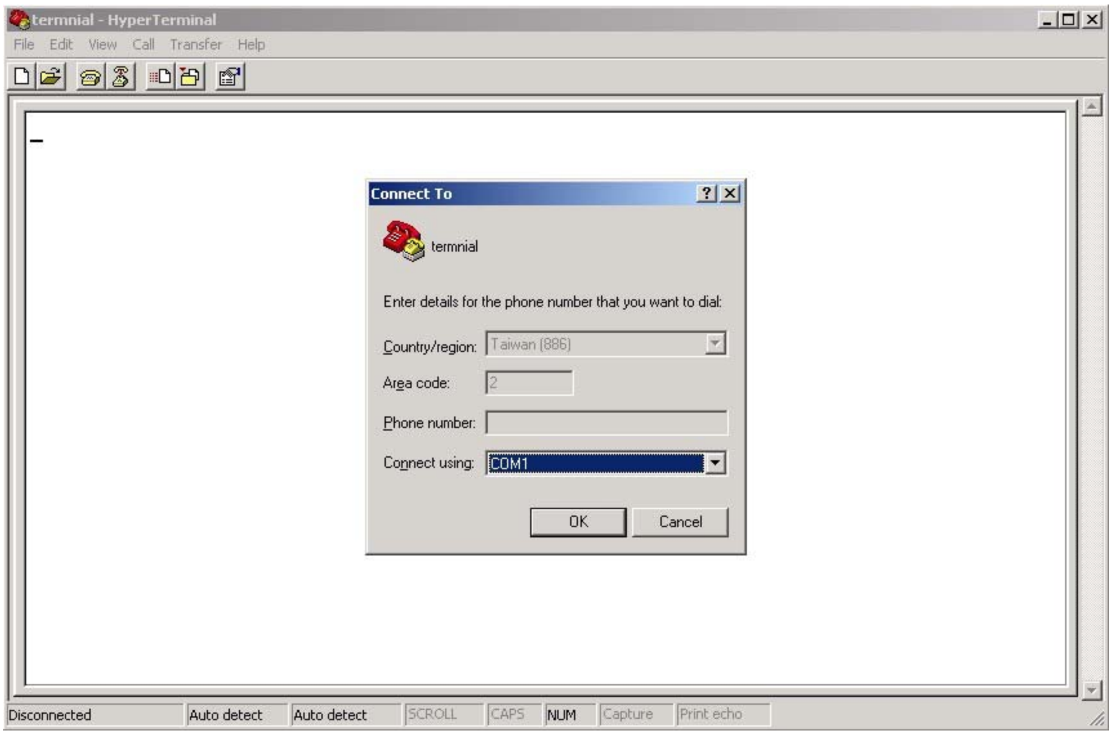

New Connection - HyperTerminal
File Edit View Call Transfer Help
Connection Description
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

Step 3. Select to use COM port number



Enter details for the phone number that you want to dial:

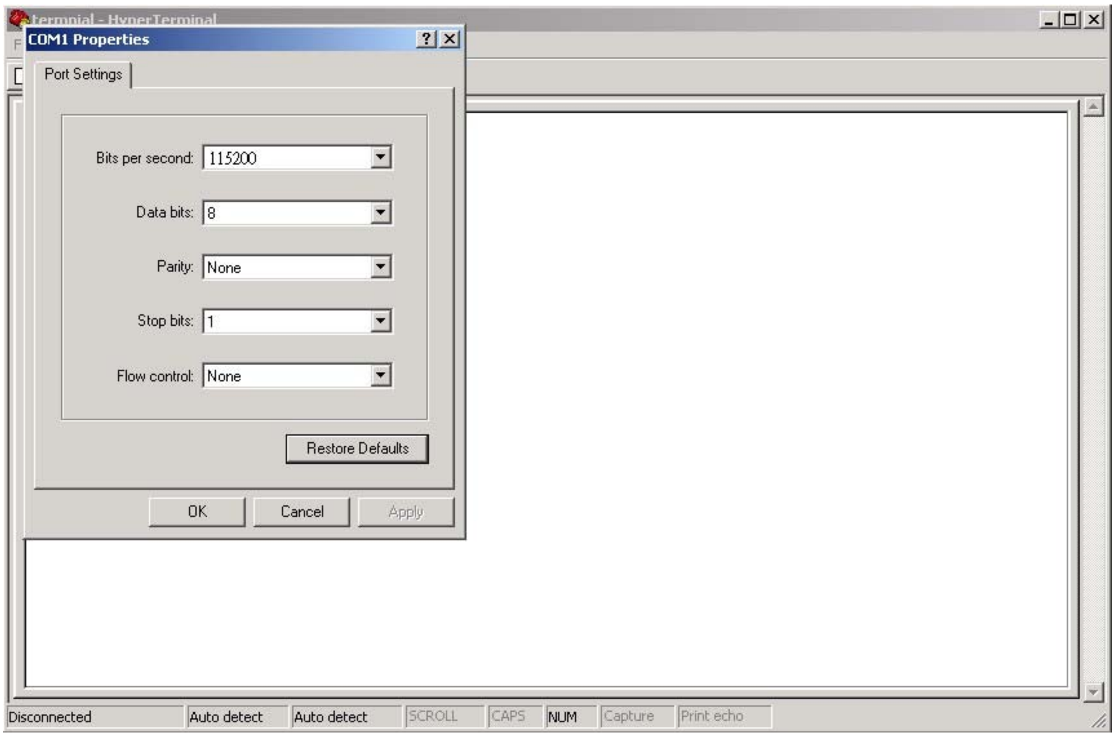
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

Step 4. The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



terminal - HyperTerminal

COM1 Properties

Port Settings

Bits per second: 115200

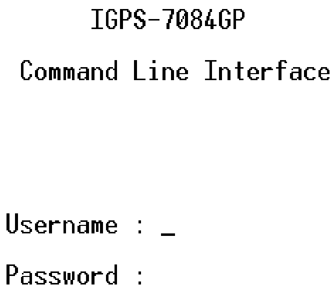
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press "**Enter**".



```
      IGPS-7084GP
Command Line Interface



Username : _
Password :
```

CLI Management by Telnet

Users can use "**TELNET**" to configure the switches.

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

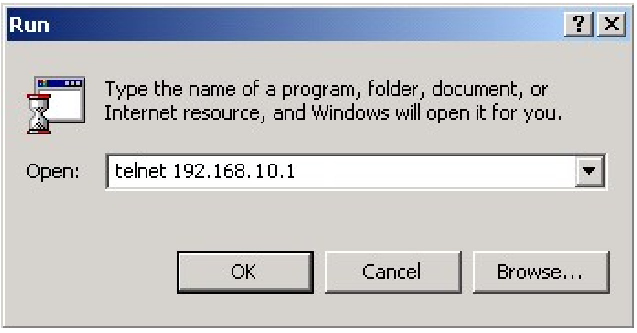
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access the console via Telnet.

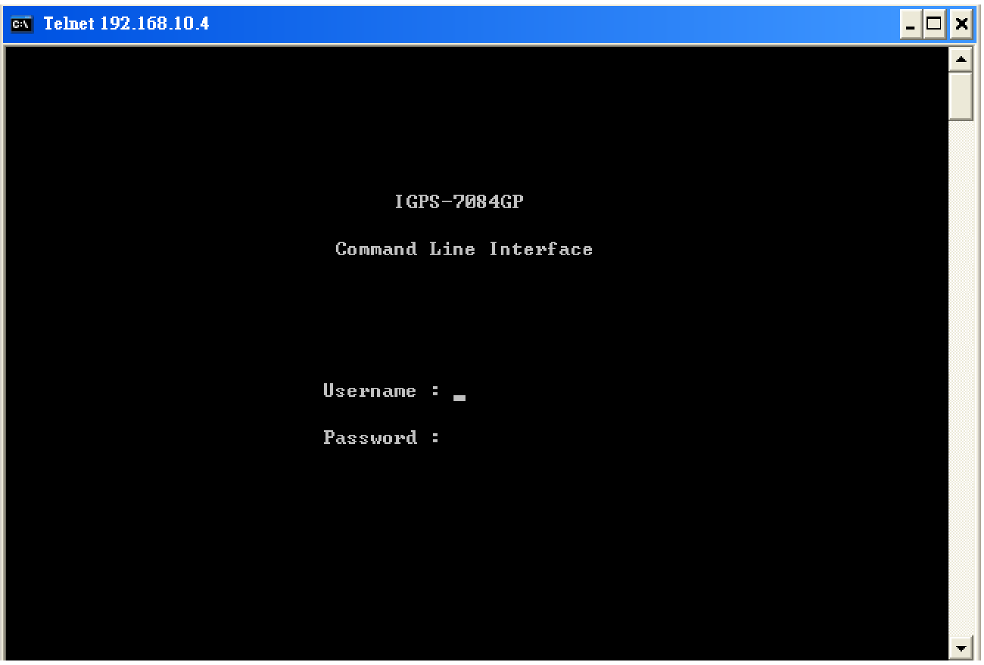
Step 1. Telnet to the IP address of the switch from the Windows "**Run**" command (or from the MS-DOS prompt) as below.



Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
OK
Cancel
Browse...

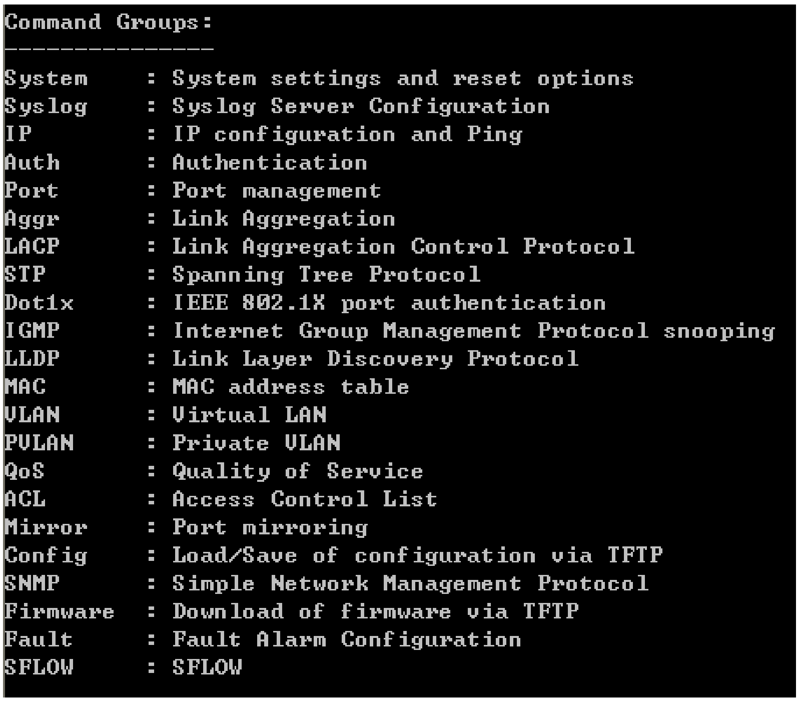
Open: telnet 192.168.10.1

Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press "**Enter**"



```
IGPS-7084GP

Command Line Interface



Username : _

Password :
```

Commander Groups



```
Command Groups:
---------------
System     : System settings and reset options
Syslog     : Syslog Server Configuration
IP         : IP configuration and Ping
Auth       : Authentication
Port       : Port management
Aggr       : Link Aggregation
LACP       : Link Aggregation Control Protocol
STP        : Spanning Tree Protocol
Dot1x      : IEEE 802.1X port authentication
IGMP       : Internet Group Management Protocol snooping
LLDP       : Link Layer Discovery Protocol
MAC        : MAC address table
VLAN       : Virtual LAN
PVLAN      : Private VLAN
QoS        : Quality of Service
ACL        : Access Control List
Mirror     : Port mirroring
Config     : Load/Save of configuration via TFTP
SNMP       : Simple Network Management Protocol
Firmware   : Download of firmware via TFTP
Fault      : Fault Alarm Configuration
SFLOW      : SFLOW
```

System

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
	Log [<log_id>] [all|info|warning|error] [clear]

Syslog

Syslog>	ServerConfiguration [<ip_addr>]

IP

IP>	Configuration
	DHCP [enable|disable]
	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]

	SNTP [<ip_addr_string>]

Auth

Auth>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Client [console|telnet|ssh|web] [none|local|radius] [enable|disable]
	Statistics [<server_index>]

Port

Port>	Configuration [<port_list>]
	State [<port_list>] [enable|disable]
	Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]
	Flow Control [<port_list>] [enable|disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable|disable|actiphy|dynamic]
	Excessive [<port_list>] [discard|restart]
	Statistics [<port_list>] [<command>]
	VeriPHY [<port_list>]

Aggr

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac|dmac|ip|port] [enable|disable]

LACP

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable]
	Key [<port_list>] [<key>]
	Role [<port_list>] [active|passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]

STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable|disable]
	bpduGuard [enable|disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

Dot1x

Dot1x>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<port_list>] [macbased|auto|authorized|unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable|disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear|eapol|radius]
	Clients [<port_list>] [all|<client_cnt>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]

IGMP

IGMP>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<vid>] [enable|disable]
	Querier [<vid>] [enable|disable]
	Fastleave [<port_list>] [enable|disable]
	Router [<port_list>] [enable|disable]
	Flooding [enable|disable]
	Groups [<vid>]
	Status [<vid>]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable|rx|tx]
	Optional_TLV [<port_list>][port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
	Interval [<interval>]
	Hold [<hold>]
	Delay [<delay>]
	Reinit [<reinit>]
	Info [<port_list>]
	Statistics [<port_list>] [clear]

MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto|disable|secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

VLAN

VLAN>	Configuration [<port_list>]
	Aware [<port_list>] [enable|disable]
	PVID [<port_list>] [<vid>|none]
	FrameType [<port_list>] [all|tagged]
	Add <vid> [<port_list>]
	Delete <vid>
	Lookup [<vid>]

PVLAN

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable|disable]

QOS

QoS>	Configuration [<port_list>]
	Classes [<class>]
	Default [<port_list>] [<class>]
	Tagprio [<port_list>] [<tag_prio>]
	QCL Port [<port_list>] [<qcl_id>]

	QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>] (etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) | (dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>) <class>
	QCL Delete <qcl_id> <qce_id>
	QCL Lookup [<qcl_id>] [<qce_id>]
	Mode [<port_list>] [strict|weighted]
	Weight [<port_list>] [<class>] [<weight>]
	Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]
	Shaper [<port_list>] [enable|disable] [<bit_rate>]
	Storm Unicast [enable|disable] [<packet_rate>]
	Storm Multicast [enable|disable] [<packet_rate>]
	Storm Broadcast [enable|disable] [<packet_rate>]

ACL

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]
	Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Delete <ace_id>
	Lookup [<ace_id>]

	Clear

Mirror

Mirror>	Configuration [<port_list>]
	Port [<port>|disable]
	Mode [<port_list>] [enable|disable|rx|tx]

Config

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable|disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included|excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip_addr_string> <file_name>

fault

Fault>	Alarm PortLinkDown [<port_list>] [enable|disable]
	Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]

SFLOW

SFLOW>	mode [enable|disable]
	version [v2|v5]
	rate [<integer>]
	interval [<integer>]
	coladdr [<ip_addr>]
	colport [<integer>]
	show

Technical Specifications

ORing Switch Model	IGPS-7084GP
Physical Ports	
10/100/1000Base-T(X) with P.S.E. ports in RJ45 Auto MDI/MDIX	**8**
1000Base-X SFP Port	**4**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T, IEEE 802.3u for 100Base-TX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T, IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol) IEEE 802.3at PoE specification (up to 30 Watts per port for P.S.E.)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 24Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Security Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH enhance network security
Jumbo Frame	Up to 9K Bytes
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 30ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping IP-based bandwidth management Application-based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Client/Server SMTP Client
Network Redundancy	O-Ring Fast Recovery Mode STP / RSTP MSTP
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED Indicators	
Power indicator	Green : Power LED x 3
R.M. indicator	Green : indicate system operated in O-Ring Master mode

Ring indicator	Green : indicate system operated in O-Ring mode
Fault indicator	Amber : Indicate excepted event occurred
10/100/1000Base-T(X) RJ45 port indicator	Green for port Link/Act.
PoE indicator	Green for PoE enable indicator
1000Base-X Fiber port indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 50~57VDC on 6-pin terminal block
Power consumption (Typ.)	20Watts (power device not included)
Overload current protection	Present
Reverse polarity protection	Not Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96.4 (W) x 108.5 (D) x 154 (H) mm (3.8 x 4.2.7 x 6.06 inch)
Weight (g)	1400g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 70°C (-40 to 158°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years